9.3

Konfigurace produktu IBM MQ

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 1053.

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

Obsah

Konfigurace produktu IBM MQ

Vytvořte jednoho či více správců front na jednom či více počítačích a nakonfigurujte je ve svých vývojových, testovacích a produkčních systémech tak, aby zpracovávaly zprávy obsahující vaše obchodní data.

Informace o této úloze

Před konfigurací produktu IBM MQsi přečtěte koncepty IBM MQ v části IBM MQ Technický přehled. Přečtěte si, jak naplánovat prostředí IBM MQ v části Plánování.

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

Pokyny, jak vytvořit, spustit, zastavit a odstranit správce front, viz “Vytvoření správců front na platformě Multiplatforms” na stránce 7.

Chcete-li získat informace o tom, jak vytvořit komponenty nezbytné pro vzájemné propojení instalací a aplikací IBM MQ , prohlédněte si téma “Konfigurace distribuovaných front” na stránce 189.

Pokyny, jak připojit klienty k serveru IBM MQ pomocí různých metod, viz “Konfigurace připojení mezi klientem a serverem” na stránce 14.

Pokyny ke konfiguraci klastru správců front naleznete v části “Konfigurace klastru správců front” na stránce 284.

Můžete změnit chování produktu IBM MQ nebo správce front změnou informací o konfiguraci. Další informace viz téma “Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83. Obecně není nutné restartovat správce front, aby se změny konfigurace projevily, s výjimkou případů uvedených v této dokumentaci produktu.

z/OS Pokyny ke konfiguraci produktu IBM MQ for z/OSnaleznete v části “Konfigurace správců front v systému z/OS” na stránce 871.

Související pojmy

IBM MQ Technický přehled

Související úlohy

Administrace lokálních objektů IBM MQ

Administrace vzdálených objektů IBM MQ

IBM i Administrace systému IBMi

z/OS Správa serveruIBM MQ for z/OS

Naplánování

z/OS Plánování prostředí IBM MQ na systému z/OS

“Konfigurace správců front v systému z/OS” na stránce 871

Pomocí těchto pokynů můžete konfigurovat správce front v systému IBM MQ for z/OS.

Multi Vytvoření správců front na platformě Multiplatforms

Než budete moci používat zprávy a fronty, musíte vytvořit a spustit alespoň jednoho správce front a jeho přidružené objekty. Správce front spravuje přidružené prostředky, zejména fronty, které vlastní. Poskytuje služby řazení do front pro aplikace pro volání rozhraní MQI (Message Queueing Interface) a příkazy pro vytváření, úpravy, zobrazování a odstraňování objektů IBM MQ .

Než začnete

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

Před vytvořením správce front je třeba zvážit několik bodů, zejména v produkčním prostředí. Projděte si následující kontrolní seznam:

Instalace přidružená ke správci front
Chcete-li vytvořit správce front, použijte IBM MQ řídicí příkaz **crtmqm**. Příkaz **crtmqm** automaticky přidruží správce front k instalaci, ze které byl vydán příkaz **crtmqm** . Pro příkazy, které pracují se správcem front, musíte zadat příkaz z instalace přidružené ke správci front. Přidruženou instalaci správce front můžete změnit pomocí příkazu setmqm . Všimněte si, že instalační program Windows nepřidá uživatele, který provádí instalaci, do skupiny mqm. Další podrobnosti viz téma Oprávnění ke správě IBM MQ na systému AIX, Linux®, and Windows.

Konvence pojmenování
V názvech používejte velká písmena, aby byla možná komunikace se správci front na všech platformách. Nezapomeňte, že jména jsou přiřazena přesně tak, jak je zadáváte. Abyste se vyhnuli nepříjemnostem při psaní, nepoužívejte zbytečně dlouhé názvy.

Zadejte jedinečný název správce front
Při vytváření správce front se ujistěte, že žádný jiný správce front nemá stejný název kdekoli v síti. Názvy správců front nejsou při vytváření správce front kontrolovány a názvy, které nejsou jedinečné, vám brání ve vytváření kanálů pro distribuované řazení do front. Pokud také používáte síť pro systém zpráv publikování/odběru, jsou odběry přidruženy k názvu správce front, který je vytvořil. Proto pokud mají správci front v klastru nebo hierarchii stejný název, může to vést k tomu, že se k nim nedostanou publikování.

Jedním ze způsobů, jak zajistit jedinečnost, je přidat před každý název správce front vlastní jedinečný název uzlu. Pokud se například uzel nazývá ACCOUNTS, můžete pojmenovat svého správce front ACCOUNTS.SATURN.QUEUE.MANAGER, kde SATURN identifikuje konkrétního správce front a QUEUE.MANAGER je rozšíření, které můžete poskytnout všem správcům front. Případně můžete toto vynechat, ale všimněte si, že ACCOUNTS.SATURN a ACCOUNTS.SATURN.QUEUE.MANAGER jsou různé názvy správců front.

Pokud používáte produkt IBM MQ pro komunikaci s jinými podniky, můžete také jako předponu uvést vlastní název podniku. To není uvedeno v příkladech, protože to znesnadňuje jejich sledování.

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

Omezit počet správců front
Můžete vytvořit tolik správců front, kolik prostředky umožňují. Protože však každý správce front vyžaduje své vlastní prostředky, je obecně lepší mít v uzlu jednoho správce front se 100 frontami, než mít deset správců front s deseti frontami.

V produkčních systémech lze mnoho procesorů využívat s jedním správcem front, ale větší serverové počítače mohou pracovat efektivněji s více správci front.

Určit výchozího správce front
Každý uzel by měl mít výchozího správce front, ačkoli je možné konfigurovat IBM MQ v uzlu bez jednoho. Výchozím správcem front je správce front, ke kterému se aplikace připojují, pokud neurčují název správce front ve volání MQCONN . Je to také správce front, který zpracovává příkazy MQSC při vyvolání příkazu `runmqsc` bez zadání názvu správce front.

Zadání správce front jako výchozí hodnoty nahradí existující specifikaci výchozího správce front pro daný uzel.

Změna výchozí správy front může ovlivnit ostatní uživatele nebo aplikace. Změna nemá žádný vliv na aktuálně připojené aplikace, protože mohou používat manipulátor z původního volání připojení v dalších voláních MQI. Tento manipulátor zajišťuje, že volání jsou směrována na stejného správce front. Všechny aplikace, které se připojují *po* změně výchozího připojení správce front k novému

výchozímu správci front. To může být to, co máte v úmyslu, ale měli byste to vzít v úvahu, než změníte výchozí nastavení.

Vytvoření výchozího správce front je popsáno v tématu "Vytvoření výchozího správce front" na stránce 11.

Určit frontu nedoručených zpráv

Fronta nedoručených zpráv je lokální fronta, do které jsou vkládány zprávy, pokud je nelze směrovat do zamýšleného místa 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 v jiném správci front, ale poskytne chybný název fronty, bude kanál zastaven a zpráva zůstane v přenosové frontě. Ostatní aplikace pak nemohou tento kanál používat pro své zprávy.

Kanály nejsou ovlivněny, pokud mají správci front fronty nedoručených zpráv. Nedoručená zpráva je vložena do fronty nedoručených zpráv na přijímacím konci, takže kanál a jeho přenosová fronta jsou k dispozici.

Při vytváření správce front zadejte název fronty nedoručených zpráv pomocí příznaku **-u** . Můžete také použít příkaz MQSC ke změně atributů správce front, který jste již definovali pro určení fronty nedoručených zpráv, která má být použita. Příklad příkazu MQSC ALTER naleznete v tématu Zobrazení a změna atributů správce front .

Určit výchozí přenosovou frontu

Přenosová fronta je lokální fronta, ve které jsou zprávy přenášené do vzdáleného správce front zařazeny do fronty před přenosem. 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 zadejte název výchozí přenosové fronty pomocí příznaku **-d** . Tím se fronta ve skutečnosti nevytváří; musíte tak učinit explicitně později. Další informace viz Práce s lokálními frontami .

Zadejte požadované parametry protokolování.

V příkazu `crtmqm` můžete zadat parametry protokolování včetně typu protokolování a cesty a velikosti souborů protokolu.

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

- Máte low-end konfiguraci systému, která nepodporuje velké protokoly.
- Očekáváte, že ve stejnou dobu bude ve frontách velký počet dlouhých zpráv.
- Očekáváte, že prostřednictvím správce front projde mnoho trvalých zpráv.

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

Další informace o parametrech protokolování viz "Konfigurace vysoké dostupnosti, zotavení a restartování" na stránce 453.

AIX **Pouze pro systémy IBM MQ for UNIX**

Před použitím příkazu **crtmqm** můžete vytvořit adresář správce front `/var/mqm/qmgrs/qmgr`, a to i v samostatném lokálním systému souborů. Pokud při použití příkazu **crtmqm**adresář `/var/mqm/qmgrs/qmgr` existuje, je prázdný a je vlastněn příkazem mqm, použije se pro data správce front. Pokud adresář není vlastněn mqm, vytvoření se nezdaří s First Failure Support Technology (FFST) zpráva. Není-li adresář prázdný, vytvoří se nový adresář.

Informace o této úloze

Chcete-li vytvořit správce front, použijte IBM MQ řídicí příkaz **crtmqm**. Další informace viz **crtmqm**. Příkaz **crtmqm** automaticky vytvoří požadované výchozí objekty a systémové objekty (viz Systémové výchozí objekty). Výchozí objekty tvoří základ všech vámi vytvořených definic objektů. Systémové objekty jsou vyžadovány pro operaci správce front.

Windows V systémech Windows máte možnost spustit více instancí správce front pomocí volby *sax* příkazu **crtmqm** .

Po vytvoření správce front a jeho objektů můžete ke spuštění správce front použít příkaz **strmqm** .

Procedura

- Informace, které vám pomohou s vytvářením a správou správců front, naleznete v následujících dílčích tématech:
  - “Vytvoření výchozího správce front” na stránce 11
  - “Nastavení existujícího správce front jako výchozího” na stránce 13
  - “Zálohování konfiguračních souborů po vytvoření správce front” na stránce 14

Související pojmy

Práce se správci front

Související úlohy

Vytvoření správce front s názvem QM1

“Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83
Úpravou informací v konfiguračních souborech (`.ini`) můžete změnit chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovoval potřebám vaší instalace. Můžete také změnit volby konfigurace pro IBM MQ MQI clients.

“Konfigurace správců front v systému z/OS” na stránce 871
Pomocí těchto pokynů můžete konfigurovat správce front v systému IBM MQ for z/OS.

Související odkazy

Systémové a výchozí objekty

crtmqm

Linux AIX Konfigurovatelný dočasný adresář

Konfigurovatelný dočasný adresář definuje umístění, do kterého by měla přejít data efemérní pro správce front. To lze použít k povolení umístění soketů domény AIX and Linux na nepřipojený systém souborů v prostředí Red Hat® OpenShift® .

Před produktem IBM MQ 9.2.0na platformách AIX and Linux jsou při spuštění správce front v adresáři `/var/mqm/sockets` vytvořeny sokety domény AIX and Linux . Při spuštění správce front v kontejneru s produktem `/var/mqm` jako připojeným systémem souborů mohou některé platformy Linux zabránit vytvoření těchto doménových soketů, protože umožňují, aby některé procesy mimo kontejner kolidovaly s operacemi uvnitř kontejneru. Tento problém brání produktu IBM MQ ve spuštění na platformě kontejneru Red Hat OpenShift pod výchozím kontextem zabezpečení.

V produktu IBM MQ 9.2.0lze atribut **EphemeralPrefix** použít ke konfiguraci umístění přechodného adresáře. Pokud tento atribut nepoužijete, neuvidíte žádné změny v chování.

Při vytvoření položky správce front v produktu `mqs.ini` (buď pomocí příkazů **crtmqm** , nebo **addmqinf**) se atribut **EphemeralPrefix** přidá, pokud:

- Nastavte atribut **DefaultEphemeralPrefix** v souboru “AllQueueSekce správců souboru mqs.ini” na stránce 89.
- Nastavte proměnnou prostředí **MQ_EPHEMERAL_PREFIX** .
- Zadejte **-v** `EphemeralPrefix` pouze pro příkaz **addmqinf** .

Můžete také explicitně přidat atribut **EphemeralPrefix** do existujícího správce front, když je zastaven, a tento atribut se přidá při restartování správce front.

Zadáte-li atribut **EphemeralPrefix** , způsobí při spuštění správce front, že se data pro správce front vytvoří pod touto předponou, nikoli pod jeho obvyklým umístěním. To znamená:

- Soubory soketů, které jsou obvykle přítomny v adresáři `/var/mqm/sockets/<QM>` , budou nyní v adresáři `/<EphemeralPrefix>/sockets/<QM>` .
- Soubory podfondu, které se obvykle nacházejí v adresáři `/<Prefix>/qmgrs/<QM>/@<Subpool>` , budou nyní v adresáři `/<EphemeralPrefix>/qmgrs/<QM>/@<Subpool>` .

Notes:

- Produkt `/var/mqm/sockets/@SYSTEM` zůstává ve svém pevném umístění a není součástí atributu **EphemeralPrefix** .
- `AMQCLCHL.TAB` zůstává pod `/<Prefix>/qmgrs/<QM>/@ipcc` a není součástí atributu **EphemeralPrefix** .

Počet znaků, které může atribut **EphemeralPrefix** obsahovat, závisí na vaší platformě:

- Linux AIX Na platformách AIX and Linux je omezena na 12 znaků.
- IBM i V systému IBM i je omezena na 24 znaků.

Pokud uvedete atribut **EphemeralPrefix** , který je příliš dlouhý nebo neexistuje, obdržíte zprávu AMQ7001E :

```
AMQ7001E: Umístění uvedené pro správce front je neplatné.
```

.

Multi Adresář uživatelských dat

K uložení stavu trvalé aplikace můžete použít adresář `userdata` .

Každý správce front IBM MQ má vyhrazený systém souborů pro svůj trvalý stav, který zahrnuje jak data fronty, tak protokol zotavení. Systém souborů obsahuje adresář `userdata` , který můžete použít k uložení informací o trvalém stavu pro vaše aplikace. Viz Obsah adresáře v systémech Unix a Linux Systems a Obsah adresáře v systémech Windows.

Adresář `userdata` může být užitečný v řadě situací, například:

- V konfiguracích RDQM tak, aby se informace o aplikaci přesunovaly i v případě, že dojde k selhání správce front, do jiného uzlu (viz “Ukládání stavu trvalé aplikace” na stránce 565).
- Pro správce front s více instancemi tak, aby jejich stav aplikace byl umístěn s jejich daty správce front ve sdíleném síťovém systému souborů.
- Obecněji, kde jsou aplikace nakonfigurovány služby správce front.

Pokud se rozhodnete uložit stav aplikace do adresáře `userdata` , musíte si uvědomit, že data zapsaná do tohoto umístění mohou spotřebovat dostupné místo na disku přidělené správci front. Je třeba zajistit, aby byl pro správce front k dispozici dostatek místa na disku pro zápis dat fronty, protokolů a dalších informací o trvalém stavu.

Adresář `userdata` má vlastnictví uživatele mqm a skupiny a je čitelný, takže k němu mohou uživatelé přistupovat, aniž by museli být ve skupině administrátorů IBM MQ (tj. mqm). Nemůžete upravit oprávnění adresáře `userdata` , ale můžete v něm vytvořit obsah s libovolným vlastnictvím a oprávněními, která požadujete.

Multi Vytvoření výchozího správce front

Výchozím správcem front je správce front, ke kterému se aplikace připojují, pokud neurčují název správce front ve volání MQCONN. Je to také správce front, který zpracovává příkazy MQSC při vyvolání příkazu

runmqsc bez zadání názvu správce front. Chcete-li vytvořit správce front, použijte IBM MQ řídicí příkaz **crtmqm**.

Než začnete

Před vytvořením výchozího správce front si přečtěte pokyny popsané v tématu “Vytvoření správců front na platformě Multiplatforms” na stránce 7.

Linux AIX Když použijete **crtmqm** k vytvoření správce front v systému AIX and Linux, pokud adresář `/var/mqm/qmgrs/qmgr` již existuje, je vlastněn mqm a je prázdný, použije se pro data správce front. Pokud adresář není vlastněn mqm, vytvoření správce front se nezdaří se zprávou First Failure Support Technology (FFST). Pokud adresář není prázdný, vytvoří se nový adresář pro data správce front.

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

Informace o této úloze

Při vytváření správce front pomocí příkazu **crtmqm** příkaz automaticky vytvoří požadované výchozí objekty a systémové objekty. Výchozí objekty tvoří základ všech definic objektů, které jste vytvořili, a systémové objekty jsou nezbytné pro operaci správce front.

Zahrnutím příslušných parametrů do příkazu můžete také definovat například název výchozí přenosové fronty, kterou má správce front používat, a název fronty nedoručených zpráv.

Windows V systému Windowsmůžete pomocí volby **sax** příkazu **crtmqm** spustit více instancí správce front.

Další informace o příkazu **crtmqm** a jeho syntaxi viz **crtmqm**.

Procedura

- Chcete-li vytvořit výchozího správce front, použijte příkaz **crtmqm** s příznakem **-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
  Název výchozí přenosové fronty, kterou má tento správce front používat.

  Poznámka: Produkt IBM MQ pro vás nevytváří výchozí přenosovou frontu; musíte ji definovat sami.

  -u SYSTEM.DEAD.LETTER.QUEUE
  Jedná se o název výchozí fronty nedoručených zpráv vytvořené produktem IBM MQ při instalaci.

  SATURN.QUEUE.MANAGER
  Jedná se o název tohoto správce front. Musí se jednat o poslední parametr zadaný v příkazu `crtmqm` .

Jak pokračovat dále

Po vytvoření správce front a jeho objektů použijte příkaz **strmqm** k Spuštění správce front.

Související pojmy
Práce s lokálními frontami

Související úlohy

"Zálohování konfiguračních souborů po vytvoření správce front" na stránce 14
Informace o konfiguraci systému IBM MQ jsou uloženy v konfiguračních souborech na systému AIX, Linux, and Windows. Po vytvoření správce front zazálohujte konfigurační soubory. Pokud pak vytvoříte jiného správce front, který způsobí problémy, můžete po odebrání zdroje problému obnovit zálohy.

Zobrazení a změna atributů správce front

Související odkazy

Systémové a výchozí objekty

Multi Nastavení existujícího správce front jako výchozího

Existujícího správce front můžete nastavit jako výchozího správce front buď ručně pomocí textového editoru, nebo v systémech Windows a Linuxpomocí IBM MQ Explorer.

Informace o této úloze

Chcete-li pomocí textového editoru nastavit existujícího správce front jako výchozího správce front, postupujte takto.

Windows Linux Na systémech Windows a Linux (x86 a x86-64), dáváte-li přednost použití produktu IBM MQ Explorer k provedení této změny, viz "Použití IBM MQ Explorer k nastavení správce front jako výchozího" na stránce 13.

Když vytvoříte výchozího správce front, jeho název se vloží do atributu `Name` sekce `DefaultQueueManager` v konfiguračním souboru IBM MQ (`mqs.ini`). Sekce a její obsah se automaticky vytvoří, pokud neexistují.

Procedura

- Chcete-li nastavit existujícího správce front jako výchozího, změňte název správce front v atributu `Name` na název nového výchozího správce front. To můžete provést ručně pomocí textového editoru.
- Pokud v uzlu nemáte výchozího správce front a chcete nastavit existujícího správce front jako výchozího, vytvořte sekci *`DefaultQueueManager`* s požadovaným názvem sami.
- Pokud omylem změníte výchozího správce front na jiného a chcete se vrátit k původnímu výchozímu správci front, upravte sekci `DefaultQueueManager` v souboru `mqs.inia` nahraďte nežádoucího výchozího správce front požadovaným správcem front.

Související úlohy

"Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms" na stránce 83
Úpravou informací v konfiguračních souborech (`.ini`) můžete změnit chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovoval potřebám vaší instalace. Můžete také změnit volby konfigurace pro IBM MQ MQI clients.

Windows Linux Použití IBM MQ Explorer k nastavení správce front jako výchozího

V systémech Windows a Linux (na platformáchx86 a x86-64) můžete pomocí produktu IBM MQ Explorer nastavit existujícího správce front jako výchozího správce front.

Informace o této úloze

Chcete-li použít produkt IBM MQ Explorer k nastavení existujícího správce front jako výchozího správce front v systémech Windows a Linux (x86 a x86-64), postupujte takto.

Chcete-li tuto změnu provést ručně pomocí textového editoru, viz "Nastavení existujícího správce front jako výchozího" na stránce 13.

Postup

1. Otevřete produkt IBM MQ Explorer.
2. Klepněte pravým tlačítkem myši na položku **IBM MQ**a vyberte volbu **Vlastnosti ...**. Zobrazí se panel **Vlastnosti produktu IBM MQ** .
3. Do pole **Výchozí název správce front** zadejte název výchozího správce front.
4. Klepněte na tlačítko **OK**.

ALW Zálohování konfiguračních souborů po vytvoření správce front

Informace o konfiguraci systému IBM MQ jsou uloženy v konfiguračních souborech na systému AIX, Linux, and Windows. Po vytvoření správce front zazálohujte konfigurační soubory. Pokud pak vytvoříte jiného správce front, který způsobí problémy, můžete po odebrání zdroje problému obnovit zálohy.

Informace o této úloze

Obecným pravidlem je zálohovat konfigurační soubory při každém vytvoření nového správce front.

Existují dva typy konfiguračního souboru:

- Při instalaci produktu se vytvoří konfigurační soubor IBM MQ (`mqs.ini`). Obsahuje seznam správců front, který je aktualizován při každém vytvoření nebo odstranění správce front. Pro každý uzel existuje jeden soubor `mqs.ini` .
- Při vytváření nového správce front se automaticky vytvoří nový konfigurační soubor správce front (`qm.ini`). Obsahuje konfigurační parametry pro správce front.

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

- Windows Na systémech Windows : `amqp_win.properties`
- Linux AIX Na systémech AIX and Linux : `amqp_unix.properties`

Související úlohy

“Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83
Úpravou informací v konfiguračních souborech (`.ini`) můžete změnit chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovoval potřebám vaší instalace. Můžete také změnit volby konfigurace pro IBM MQ MQI clients.

“Zálohování a obnova dat správce front IBM MQ” na stránce 650
Správce front můžete chránit před možným poškozením způsobeným selháním hardwaru zálohováním správců front a dat správců front, zálohováním pouze konfigurace správce front a použitím záložního správce front.

Konfigurace připojení mezi klientem a serverem

Chcete-li konfigurovat komunikační spojení mezi produktem IBM MQ MQI clients a servery, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

Informace o této úloze

V systému IBM MQse logická komunikační spojení mezi objekty nazývají *kanály*. Kanály používané pro připojení produktu IBM MQ MQI clients k serverům se nazývají kanály MQI. Definice kanálů se nastavují na každém konci odkazu tak, aby aplikace IBM MQ v produktu IBM MQ MQI client mohla komunikovat se správcem front na serveru.

Před definováním kanálů MQI se musíte rozhodnout, jakou formu komunikace budete používat, a definovat připojení na obou koncích kanálu.

Pokud definujete kanál MQI mezi produktem IBM MQ MQI client a správcem front, který se nacházejí v různých fyzických sítích, nebo který komunikuje prostřednictvím brány firewall, může použití produktu IBM MQ Internet Pass-Thru zjednodušit konfiguraci. Další informace naleznete v tématu IBM MQ Internet Pass-Thru.

Postup

1. Rozhodněte se, jakou formu komunikace budete používat.
   Viz “Jaký typ komunikace použít” na stránce 15.
2. Definujte připojení na obou koncích kanálu.
   Chcete-li definovat připojení, musíte:
   a) Nakonfigurujte připojení.
   b) Zaznamenejte hodnoty parametrů, které potřebujete pro definice kanálů.
   c) Povolte serveru zjišťovat příchozí síťové požadavky z produktu IBM MQ MQI clientspuštěním *modulu listener*.

Související pojmy

“IBM MQ MQI client konfigurační soubor mqclient.ini” na stránce 155
Klienty můžete konfigurovat pomocí atributů v textovém souboru. Tyto atributy mohou být přepsány proměnnými prostředí nebo jinými způsoby specifickými pro platformu.

Související úlohy

“Použití proměnných prostředí IBM MQ” na stránce 61
Pomocí příkazů můžete zobrazit aktuální nastavení nebo resetovat hodnoty proměnných prostředí IBM MQ .

Připojení aplikací klienta produktu IBM MQ MQI ke správcům front

Související odkazy

ZOBRAZIT CHLAUTH

NASTAVIT CHLAUTH

Jaký typ komunikace použít

Různé platformy podporují různé komunikační protokoly. Vaše volba přenosového protokolu závisí na vaší kombinaci platformy IBM MQ MQI client a platformy serveru.

Typy přenosových protokolů pro kanály MQI

V závislosti na platformách klienta a serveru existují pro kanály MQI až čtyři typy přenosových protokolů:

- TCP/IP
- LU 6.2
- NetBIOS
- SPX

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 systém IBM MQ MQI clientsmůže být užitečné mít alternativní kanály MQI používající různé přenosové protokoly.

Volba přenosového protokolu závisí také na konkrétní kombinaci platforem klienta a serveru IBM MQ . Možné kombinace jsou uvedeny v následující tabulce.

Tabulka 1. Přenosové protokoly-kombinace platforem IBM MQ MQI client a serverů		
Přenosový protokol	**IBM MQ MQI client**	**Server IBM MQ**
TCP/IP "1" na stránce 16	IBM i IBM i AIX AIX Linux Linux Windows Windows	IBM i IBM i AIX AIX Linux Linux Windows Windows z/OS z/OS
LU 6.2	AIX AIX Linux Linux"2" na stránce 16 Windows Windows	IBM i IBM i AIX AIX Linux Linux"2" na stránce 16 Windows Windows z/OS z/OS
NetBIOS	Windows Windows	Windows Windows
SPX	Windows Windows	Windows Windows

Notes:

1. MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Viz Definování Aspera gateway připojení na Linux nebo Windows.
2. Kromě Linux (platforma POWER)

Související pojmy

"Definování připojení TCP na systému Windows" na stránce 251
Definujte připojení TCP konfigurací kanálu na odesílajícím konci tak, aby určoval adresu cíle, a spuštěním programu modulu listener na přijímajícím konci.

"Definování připojení TCP na systému AIX and Linux" na stránce 258
Definice kanálu na odesílajícím konci určuje adresu cíle. Modul listener nebo démon inet je konfigurován pro připojení na přijímacím konci.

"Definování připojení TCP na systému IBM i" na stránce 277
Můžete definovat připojení TCP v rámci definice kanálu pomocí pole Název připojení.

"Definování připojení TCP na systému z/OS" na stránce 971
Chcete-li definovat připojení TCP, existuje řada nastavení, která se mají konfigurovat.

"Definování připojení LU 6.2 na systému Windows" na stránce 252
Architektura SNA musí být konfigurována tak, aby bylo možné mezi těmito dvěma počítači navázat konverzaci LU 6.2 .

"Definování připojení LU 6.2 na systému AIX and Linux" na stránce 262
Architektura SNA musí být konfigurována tak, aby bylo možné mezi těmito dvěma počítači navázat konverzaci LU 6.2 .

"Definování připojení LU 6.2 na systému IBM i" na stránce 279

Definujte podrobnosti komunikace LU 6.2 pomocí jména režimu, jména TP a jména připojení plně kvalifikovaného připojení LU 6.2 .

“Definování připojení NetBIOS na systému Windows” na stránce 254
Připojení NetBIOS se vztahuje pouze na klienta a server, na kterém běží produkt Windows. Produkt IBM MQ používá při vytváření připojení NetBIOS k jinému produktu IBM MQ tři typy prostředků NetBIOS : relace, příkazy a názvy. Každý z těchto prostředků má limit, který je nastaven buď standardně, nebo podle volby během instalace systému NetBIOS.

Související úlohy

“Definování připojení Aspera gateway na platformách Linux nebo Windows” na stránce 822
Produkt IBM Aspera faspio Gateway poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě IBM MQ. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows.

Související odkazy

“Omezení připojení TCP/IP” na stránce 17
Počet neprovedených požadavků na připojení, které lze zařadit do fronty na jednom portu TCP/IP, závisí na platformě. Dojde-li k dosažení limitu, dojde k chybě.

“Definování připojení LU6.2 pro z/OS pomocí APPC/MVS” na stránce 974
Chcete-li definovat připojení LU6.2 , existuje řada nastavení, která se mají konfigurovat.

Omezení připojení TCP/IP

Počet neprovedených požadavků na připojení, které lze zařadit do fronty na jednom portu TCP/IP, závisí na platformě. Dojde-li k dosažení limitu, dojde k chybě.

Tento limit připojení není stejný jako maximální počet klientů, které můžete připojit k serveru IBM MQ . K serveru můžete připojit více klientů až do úrovně určené systémovými prostředky serveru. Hodnoty nevyřízených požadavků na připojení jsou uvedeny v následující tabulce:

Tabulka 2. Maximální počet nevyřízených požadavků na připojení zařazených do fronty na portu TCP/IP

Platforma serveru	**Maximální počet požadavků na připojení**
AIX AIX	100
Linux Linux	100
IBM i IBM i	255
Windows Windows Server	100
Windows Windows Pracovní stanice	100
z/OS z/OS	255

Pokud je dosažen limit připojení, klient obdrží návratový kód MQRC_HOST_NOT_AVAILABLE z volání `MQCONN` a chybu AMQ9202 v protokolu chyb klienta (`/var/mqm/errors/AMQERR0n.LOG` v systémech AIX and Linux nebo `amqerr0n.log` v podadresáři chyb instalace klienta IBM MQ v systému Windows). Pokud klient zopakuje požadavek `MQCONN` , může být úspěšný.

Chcete-li zvýšit počet požadavků na připojení, které můžete provést, a vyhnout se generování chybových zpráv pomocí tohoto omezení, můžete mít více modulů listener, z nichž každý naslouchá na jiném portu, nebo mít více než jednoho správce front.

Jak nastavit IBM MQ MQI client

Při nastavování klienta postupujte podle těchto pokynů.

Než začnete

Chcete-li nastavit server IBM MQ MQI client , musíte mít již nainstalovaný a funkční server IBM MQ , ke kterému se bude klient připojovat.

Postup

1. Zkontrolujte, zda máte vhodnou platformu pro klienta MQI produktu IBM MQ a zda hardware a software splňují požadavky.

   Podpora platformy je popsána v tématu Podpora platformy pro IBM MQ klienty.
2. Rozhodněte, jak budete instalovat produkt IBM MQ na pracovní stanici klienta, a poté postupujte podle pokynů pro konkrétní kombinaci platforem klienta a serveru.

   Instalace je popsána v následujících tématech:

   - 

     Instalace klienta IBM MQ v systému AIX
   - 

     Instalace klienta IBM MQ na Linux
   - 

     Instalace klienta IBM MQ na Windows
   - 

     Instalace klienta IBM MQ na IBM i
3. Ujistěte se, že jsou vaše komunikační spojení nakonfigurovaná a připojená.

   Konfigurace komunikačních spojů je popsána v tématu Konfigurace připojení mezi serverem a klientem.
4. Zkontrolujte, zda vaše instalace pracuje správně.

   Prohlédněte si sekci verifikace instalačního postupu pro platformu nebo platformy, které váš podnik používá.
5. Když máte ověřenou instalaci produktu IBM MQ MQI client , zvažte, zda musíte zabezpečit svého klienta.

   Zabezpečení klienta je popsáno v tématu Nastavení IBM MQ MQI client zabezpečení.
6. Nastavte kanály mezi klientem MQI IBM MQ a serverem, které jsou vyžadovány aplikacemi IBM MQ , které chcete spustit na klientovi.

   Nastavení kanálů je popsáno v tématu Definování kanálů MQI. Používáte-li protokol TLS, je třeba vzít v úvahu několik dalších aspektů.

   Tyto aspekty jsou popsány v tématu Určení, že kanál MQI používá protokol TLS. Možná budete muset použít konfigurační soubor IBM MQ MQI client nebo proměnné prostředí IBM MQ k nastavení kanálů. IBM MQ proměnné prostředí jsou popsány v tématu Použití IBM MQ proměnných prostředí.
7. Úplný popis aplikací IBM MQ naleznete v tématu Vývoj aplikací .
8. Při návrhu, sestavování a spouštění aplikací v prostředí IBM MQ MQI client je třeba vzít v úvahu rozdíly oproti prostředí správce front.

   Informace o těchto rozdílech viz:

   - Použití rozhraní fronty zpráv (MQI) v klientské aplikaci
   - Sestavení aplikací pro IBM MQ MQI clients
   - Připojení IBM MQ MQI client aplikací ke správcům front
   - Řešení problémů s produktem IBM MQ MQI clients

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 podporujících standard XA, například CICS a Tuxedo.

Windows **Microsoft Transakční server (pouze systémyWindows)**
Pouze v systémech Windows podporuje rozhraní správce prostředků XA také server Microsoft Transaction Server (MTS). Podpora IBM MQ MTS dodávaná s rozšířeným transakčním klientem poskytuje most mezi MTS a rozhraním správce prostředků XA.

WebSphere Application Server
Produkt WebSphere Application Server 6 a novější obsahuje poskytovatele systému zpráv IBM MQ , takže nemusíte používat rozšířeného transakčního klienta.

Konfigurace správců transakcí vyhovujících standardu XA

Nejprve nakonfigurujte základního klienta IBM MQ a poté pomocí informací v těchto tématech nakonfigurujte rozšířenou transakční funkci.

Poznámka: Tento oddíl předpokládá, že máte základní informace o rozhraní XA publikovaném skupinou The Open Group v části *Distributed Transaction Processing: The XA Specification*.

Chcete-li konfigurovat rozšířeného transakčního klienta, musíte nejprve nakonfigurovat základního klienta IBM MQ , jak je popsáno v tématu:

- AIX Instalace klienta IBM MQ na AIX
- Linux Instalace klienta IBM MQ na Linux
- Windows Instalace klienta IBM MQ na Windows
- IBM i Instalace klienta IBM MQ na IBM i

Pomocí informací pro vaši platformu pak můžete nakonfigurovat rozšířenou transakční funkci pro správce transakcí kompatibilního s podporou XA, jako např. CICS a Tuxedo.

Správce transakcí komunikuje se správcem front jako se správcem prostředků pomocí stejného kanálu MQI, který používá klientská aplikace připojená ke správci front. Když správce transakcí vydá volání funkce správce prostředků (xa_), použije se kanál MQI k předání volání správci front a k přijetí výstupu ze správce front zpět.

Buď může správce transakcí 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 aplikace klienta později zavolá MQCONN nebo MQCONNX ve stejném podprocesu, volání MQCONN nebo MQCONNX se úspěšně dokončí a aplikaci se vrátí manipulátor připojení. Aplikace neobdrží kód dokončení MQCC_WARNING s kódem příčiny MQRC_ALREADY_CONNECTED.
- Pokud aplikace klienta spustí kanál MQI a správce transakcí později zavolá xa_open ve stejném podprocesu, bude volání xa_open předáno správci front pomocí kanálu MQI.

V situaci zotavení po selhání může správce transakcí v případě, že nejsou spuštěny žádné klientské aplikace, použít vyhrazený kanál MQI k obnovení neúplných pracovních jednotek, v nichž se správce front účastnil v době selhání.

Při použití rozšířeného transakčního klienta se správcem transakcí kompatibilním s podporou XA mějte na paměti následující podmínky:

- V rámci jednoho podprocesu může být klientská aplikace v daném okamžiku připojena pouze k jednomu správci front. Toto omezení platí pouze v případě použití rozšířeného transakčního klienta; klientská aplikace, která používá základního klienta IBM MQ , může být připojena k více než jednomu správci front souběžně v rámci jednoho podprocesu.
- Každý podproces klientské aplikace se může připojit k jinému správci front.

- Klientská aplikace nemůže používat sdílené obslužné rutiny připojení.

Chcete-li konfigurovat rozšířenou transakční funkci, musíte správci transakcí pro každého správce front, který vystupuje jako správce prostředků, poskytnout následující informace:

- Řetězec xa_open
- Ukazatel na strukturu přepínače XA

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

- Spuštění kanálu MQI pro správce front serveru v případě, že klientská aplikace dosud nespustila kanál MQI.
- Chcete-li zkontrolovat, že správce front, kterého správce transakcí otevře jako správce prostředků, je stejný jako správce front, ke kterému se připojuje klientská aplikace.
- Chcete-li vyhledat funkce ax_reg a ax_unreg správce transakcí, pokud správce front používá dynamickou registraci

Formát řetězce xa_open a další podrobnosti o tom, jak jsou informace v řetězci xa_open používány rozšířeným transakčním klientem, viz “Formát řetězce xa_open” na stránce 21.

Struktura přepínače XA umožňuje správci transakcí vyhledat funkce xa _ poskytované rozšířeným transakčním klientem a určuje, zda správce front používá dynamickou registraci. Informace o strukturách přepínačů XA dodávaných s rozšířeným transakčním klientem naleznete v části “Struktury přepínačů XA” na stránce 25.

Chcete-li získat informace o tom, jak konfigurovat rozšířenou funkci transakcí pro konkrétního správce transakcí a další informace o použití správce transakcí s rozšířeným klientem transakcí, prohlédněte si následující sekce:

- “Konfigurace rozšířeného transakčního klienta pro CICS” na stránce 26
- “Konfigurace rozšířeného transakčního klienta pro produkt Tuxedo” na stránce 27

Související pojmy

“Parametry CHANNEL, TRPTYPE, CONNAME a QMNAME řetězce xa_open” na stránce 23
Pomocí těchto informací zjistíte, jak rozšířený transakční klient používá tyto parametry k určení správce front, ke kterému se má připojit.

“Další chyba zpracování pro xa_open” na stránce 24
Volání xa_open za určitých okolností selhává.

Související úlohy

“Použití rozšířeného transakčního klienta s kanály TLS” na stránce 25
Kanál TLS nelze nastavit pomocí řetězce xa_open. Chcete-li použít tabulku definic kanálů klienta (ccdt), postupujte podle těchto pokynů.

Související odkazy

“Parametry TPM a AXLIB” na stránce 24
Rozšířený transakční klient používá parametry TPM a AXLIB k vyhledání funkcí ax_reg a ax_unreg správce transakcí. Tyto funkce se používají pouze v případě, že správce front používá dynamickou registraci.

“Zotavení po selhání v rozšířeném transakčním zpracování” na stránce 24
Po selhání musí být správce transakcí schopen obnovit všechny nedokončené jednotky práce. Chcete-li tak učinit, musí být správce transakcí schopen otevřít jako správce prostředků libovolného správce front, který se v době selhání účastnil nedokončené pracovní jednotky.

z/OS *Aspekty produktu IBM MQ for z/OS pro rozšířená transakční připojení klienta*

Někteří správci transakcí XA používají posloupnosti volání koordinace transakcí, které jsou nekompatibilní s funkcemi běžně dostupnými klientům připojujícím se k produktu IBM MQ for z/OS.

Je-li zjištěna nekompatibilní posloupnost, produkt IBM MQ for z/OS může pro připojení vydat nevhodné ukončení a vrátit klientovi chybovou odezvu.

Například `xa_prepare` přijímá nestandardnímu konci 5C6-00D4007Ds návratovým kódem -3 (XAER_RMERR) vráceným klientovi.

Dalším příkladem je, že `xa_end` přijímá nestandardni ukončení 5C6-00D40079.

Pro správce transakcí, kteří se s touto situací setkají, proveďte následující akci, abyste správci transakcí umožnili interakci s produktem IBM MQ for z/OS.

Ujistěte se, že jste povolili změny připojení klienta XA na systému IBM MQ for z/OS , které umožňují správci transakcí připravit transakci na jiném připojení.

Notes:

- Změna není standardně povolena. Chcete-li použít změnu, musíte zadat klíčové slovo CSQSERVICE1 (velkými písmeny) kdekoli v poli popisu kanálu SVRCONN používaného klientem XA.
- Kanály s klíčovým slovem CSQSERVICE1 mají následující omezení:
  - Dispozice jednotky zotavení GROUP není povolena. Je povolena pouze jednotka odebrání zotavení QMGR . Dispozice je určena názvem zadaným ve volání `xa_open` . Je-li použit název skupiny sdílení front, vyžádá si připojení XA skupinovou jednotku zotavení.

    Volání `xa_open` určující název skupiny sdílení front v parametru **`xa_info`** se nezdaří s volbou *xaer_inval*.
  - Volby *MQGMO_LOCK* a *MQGMO_UNLOCK* nejsou povoleny. Volání MQGET s parametrem *MQGMO_LOCK* nebo *MQGMO_UNLOCK* se nezdařilo s chybou MQRC_ENVIRONMENT_ERROR.

Změna byla povolena v produktu IBM MQ for z/OS 9.0 prostřednictvím APAR P173410

Související pojmy

“Konfigurace správců transakcí vyhovujících standardu XA” na stránce 19
Nejprve nakonfigurujte základního klienta IBM MQ a poté pomocí informací v těchto tématech nakonfigurujte rozšířenou transakční funkci.

Formát řetězce xa_open

Řetězec xa_open obsahuje dvojice definovaných názvů a hodnot parametrů.

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 nerozlišují velikost písmen, ale pokud není uvedeno jinak, hodnoty parametrů rozlišují 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. Následující protokoly jsou platné hodnoty:

LU62
LU SNA 6.2

NETBIOS
NetBIOS

SPX
IPX/SPX

TCP
TCP/IP

Jedná se o volitelný parametr. Pokud je vynechán, předpokládá se předvolená hodnota TCP. Hodnoty parametru nerozlišují velikost písmen.

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

LU62
Symbolický název místa určení, který identifikuje položku informací o připojení CPI-C.

Síťové kvalifikované jméno partnerské LU není platnou hodnotou ani aliasem partnerské LU. Důvodem je, že neexistují žádné další parametry pro uvedení názvu transakčního programu (TP) a názvu režimu.

NETBIOS
Název NetBIOS .

SPX
4bajtová síťová adresa, 6bajtová adresa uzlu a volitelné 2bajtové číslo soketu. Tyto hodnoty musí být uvedeny v hexadecimální notaci. Adresa sítě a uzlu musí být oddělena tečkou a číslo soketu, je-li zadáno, musí být uzavřeno v závorkách. Příklad:

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

Pokud je číslo soketu vynecháno, předpokládá se výchozí hodnota 5e86 .

TCP
Název hostitele nebo adresa IP, volitelně následované číslem portu v závorkách. Pokud je číslo portu vynecháno, předpokládá se výchozí hodnota 1414. Více hostitelů a portů pro správce front lze zadat pomocí středníku, například:

```
host1(1415);host2(1416);host3(1417)
```

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

QMNAME
Název správce front na konci serveru kanálu MQI. Název nesmí být prázdný ani nesmí začínat hvězdičkou (*), ani nesmí začínat hvězdičkou. To znamená, že parametr musí identifikovat specifického správce front podle názvu.

Jedná se o povinný parametr.

Je-li klientská aplikace připojena ke specifickému správci front, musí být zotavení transakcí zpracováno stejným správcem front.

Pokud se aplikace připojuje ke správci front z/OS , může zadat buď název specifického správce front, nebo název skupiny sdílení front (QSG). Pomocí názvu správce front nebo názvu skupiny sdílení front řídí aplikace, zda se podílí na transakci s dispozicí zotavení jednotky QMGR nebo dispozicí zotavení jednotky GROUP. Dispoziční jednotka obnovy GROUP umožňuje zpracování obnovy transakce na libovolném členu skupiny QSG. Chcete-li použít jednotky zotavení GROUP, musí být povolen atribut správce front **GROUPUR** .

z/OS Další informace o použití jednotky zotavení GROUP naleznete v tématu Dispozice jednotky zotavení ve skupině sdílení front.

TPM:
Používaný správce transakcí. 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 parametru nerozlišují velikost písmen.

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

Jedná se o volitelný parametr.

Identifikátor UID
ID uživatele, které je poskytnuto správci front pro ověření. Je-li tento parametr zadán, musí být zadán také parametr **PWD** . Pokud je zadané ID uživatele a heslo ověřeno, použije se ID uživatele pro identifikaci připojení správce transakcí produktu ths. ID uživatele a heslo naplní objekt MQCSP ve volání MQCONNX.

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

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

Varování: V některých případech bude heslo ve struktuře MQCSP pro klientskou aplikaci odesláno v síti jako prostý text. Chcete-li se ujistit, že jsou hesla aplikací klienta řádně chráněna, prohlédněte si téma IBM MQOchrana hesel CSP.

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

Pomocí těchto informací zjistíte, jak rozšířený transakční klient používá tyto parametry k určení správce front, ke kterému se má připojit.

Pokud jsou parametry **CHANNEL** a **CONNAME** zadány v řetězci xa_open, rozšířený transakční klient použije tyto parametry a parametr **TRPTYPE** ke spuštění kanálu MQI pro správce front serveru.

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

V každém z těchto případů rozšířený transakční klient kontroluje, zda je hodnota parametru **QMNAME** název správce front na konci serveru kanálu MQI. Pokud není, volání xa_open selže a správce transakcí nahlásí selhání aplikaci.

z/OS Pokud aplikace v poli parametru **QMNAME** používá název skupiny sdílení front a vlastnost GROUPUR je ve správci front, ke kterému se připojuje, zakázána, volání xa_open selže.

z/OS Pokud se aplikační klient připojuje ke správci front z/OS , může zadat název skupiny sdílení front (QSG) pro parametr **QMNAME** . To umožňuje aplikačnímu klientovi podílet se na transakci s dispozicí pro zotavení jednotky GROUP. Další informace o dispoziční jednotce zotavení GROUP naleznete v tématu Dispozice jednotky zotavení.

Když aplikace klienta později zavolá MQCONN nebo MQCONNX ve stejném podprocesu, který správce transakcí použil k zadání 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** ve volání MQCONN nebo MQCONNX názvem správce front na konci serveru kanálu MQI. Pokud není, volání MQCONN nebo MQCONNX se nezdaří s kódem příčiny MQRC_ANOTHER_Q_MGR_CONNECTED. Pokud je hodnota parametru **QMgrName** prázdná nebo jednotlivá hvězdička (*) nebo začíná hvězdičkou, volání MQCONN nebo MQCONNX selže s kódem příčiny MQRC_Q_MGR_NAME_ERROR.

Pokud aplikace klienta již spustila kanál MQI voláním MQCONN nebo MQCONNX před voláním správce transakcí xa_open ve stejném podprocesu, použije správce transakcí místo toho tento kanál MQI. Druhý kanál MQI není spuštěn. Rozšířený transakční klient kontroluje, zda hodnota parametru **QMNAME** v řetězci xa_open je název správce front serveru. Pokud není, volání xa_open selže.

Pokud aplikace klienta nejprve spustí kanál MQI, hodnota parametru **QMgrName** ve volání MQCONN nebo MQCONNX může být prázdná nebo může začínat hvězdičkou (*). Za těchto okolností je však nutné zajistit, aby správce front, ke kterému se aplikace připojuje, byl stejný jako správce front, kterého má správce transakcí v úmyslu otevřít jako správce prostředků při pozdějším volání xa_open ve stejném podprocesu. Může se tedy vyskytnout méně problémů, pokud hodnota parametru *QMgrName* identifikuje správce front explicitně podle názvu.

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.

Pokud je parametr TPM zadán v řetězci xa_open, ale není zadán parametr AXLIB, rozšířený transakční klient předpokládá hodnotu parametru AXLIB na základě hodnoty parametru TPM. Předpokládané hodnoty parametru AXLIB viz Tabulka 3 na stránce 24 .

Tabulka 3. Předpokládané hodnoty parametru AXLIB

Hodnota čipu TPM	**Platforma**	**Předpokládaná hodnota AXLIB**
CICS	AIX	/usr/lpp/encina/lib/libEncServer.a(EncServer_shr.o)
CICS	Windows systémy	libEncServer
Tuxedo	AIX	/usr/lpp/tuxedo/lib/libtux.a(libtux.so.60)
Tuxedo	Windows systémy	libtux

Pokud je parametr AXLIB zadán v řetězci xa_open, rozšířený transakční klient použije svou hodnotu k přepsání jakékoli předpokládané hodnoty na základě hodnoty parametru TPM. Parametr AXLIB lze také použít pro správce transakcí, pro kterého parametr TPM nemá uvedenou hodnotu.

Další chyba zpracování pro xa_open

Volání xa_open za určitých okolností selhává.

Témata v této sekci popisují situace, kdy volání xa_open selže. Také selže, pokud dojde k některé z následujících situací:

- Řetězec xa_open obsahuje chyby.
- Pro spuštění kanálu MQI není k dispozici dostatek informací.
- Při pokusu o spuštění kanálu MQI došlo k problému (například správce front serveru není spuštěn).

Zotavení po selhání v rozšířeném transakčním zpracování

Po selhání musí být správce transakcí schopen obnovit všechny nedokončené jednotky práce. Chcete-li tak učinit, musí být správce transakcí schopen otevřít jako správce prostředků libovolného správce front, který se v době selhání účastnil nedokončené pracovní jednotky.

Proto se musíte ujistit, že všechny nedokončené jednotky práce byly vyřešeny, než provedete změny v jakýchkoli informacích o konfiguraci.

Případně je třeba zajistit, aby změny konfigurace neovlivňovaly schopnost správce transakcí otevřít správce front, které je třeba otevřít. Zde jsou příklady takových změn konfigurace:

- Změna obsahu řetězce xa_open

- Změna hodnoty proměnné prostředí MQSERVER
- Změna položek v tabulce CCDT (Client Channel Definition Table)
- Odstranění definice kanálu připojení serveru

Struktury přepínačů XA

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

Tyto spínací struktury jsou:

MQRMIXASwitch
Tuto strukturu přepínače používá správce transakcí, pokud správce front, který vystupuje jako správce prostředků, nepoužívá dynamickou registraci.

MQRMIXASwitchDynamic
Tuto strukturu přepínače používá správce transakcí, když správce front, který vystupuje jako správce prostředků, používá dynamickou registraci.

Tyto struktury přepínače jsou umístěny v knihovnách zobrazených v části Tabulka 4 na stránce 25.

Tabulka 4. Knihovny IBM MQ obsahující struktury přepínače XA

Platforma	**Knihovna obsahující struktury přepínače XA**
AIX AIX Linux Linux	*MQ_INSTALLATION_PATH*/lib/libmqcxa
Windows Windows systémy	*MQ_INSTALLATION_PATH*\bin\mqcxa.dll [1]

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

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

Související pojmy

“Dynamická registrace a rozšířené transakční zpracování” na stránce 25
Použití dynamické registrace je formou optimalizace, protože může snížit počet volání funkce xa _ vydaných správcem transakcí.

Dynamická registrace a rozšířené transakční zpracování
Použití dynamické registrace je formou optimalizace, protože může snížit počet volání funkce xa _ vydaných správcem transakcí.

Pokud správce front nepoužívá dynamickou registraci, zahrne správce transakcí správce front do každé pracovní jednotky. Správce transakcí to provede voláním xa_start, xa_end a xa_prepare, a to i v případě, že správce front nemá žádné prostředky aktualizované v rámci pracovní jednotky.

Pokud správce front používá dynamickou registraci, spustí se správce transakcí za předpokladu, že správce front není zapojen do transakce a nevolá xa_start. Správce front se poté zapojí do pracovní jednotky pouze v případě, že jsou jeho prostředky aktualizovány v rámci řízení synchronizačního bodu. Pokud k tomu dojde, klient rozšířené transakce zavolá ax_reg, aby zaregistroval zapojení správce front.

Použití rozšířeného transakčního klienta s kanály TLS

Kanál TLS nelze nastavit pomocí řetězce xa_open. Chcete-li použít tabulku definic kanálů klienta (ccdt), postupujte podle těchto pokynů.

Informace o této úloze

Vzhledem k omezené velikosti řetězce xa_open xa_info není možné předat všechny informace potřebné k nastavení kanálu TLS pomocí metody řetězce xa_open pro připojení ke správci front. Proto musíte buď použít tabulku definic kanálů klienta, nebo, pokud to správce transakcí povolí, vytvořit kanál s MQCONNX před zadáním volání xa_open.

Chcete-li použít tabulku definic kanálů klienta, postupujte takto:

Postup

1. Zadejte řetězec xa_open obsahující pouze povinný parametr qmname (název správce front), například: `XA_Open_String=qmname=MYQM`
2. Pomocí správce front definujte kanál CLNTCONN (připojení klienta) s požadovanými parametry TLS. Do atributu QMNAME v definici CLNTCONN zadejte název správce front. Tato hodnota bude porovnána s názvem qmname v řetězci xa_open.
3. Zpřístupněte definici CLNTCONN pro klientský systém v tabulce CCDT (Client Channel Definition Table) nebo v systému Windowsve službě Active Directory.
4. Používáte-li tabulku CCDT, identifikujte tabulku CCDT obsahující definici kanálu CLNTCONN pomocí proměnných prostředí MQCHLLIB a MQCHLTAB. Nastavte tyto proměnné v prostředích používaných klientskou aplikací i správcem transakcí.

Výsledky

To poskytne správci transakcí definici kanálu příslušnému správci front s atributy TLS potřebnými pro správné ověření, včetně SSLCIPH, CipherSpec.

Konfigurace rozšířeného transakčního klienta pro CICS

Rozšířeného transakčního klienta pro použití produktem CICS nakonfigurujete přidáním definice prostředku XAD do oblasti CICS .

Přidejte definici prostředku XAD pomocí příkazu CICS resource definition online (RDO) **cicsadd**. Definice prostředku XAD určuje následující informace:

- Řetězec xa_open
- Úplný název cesty k souboru načtení přepínače

Jeden soubor načtení přepínače je dodáván pro použití produktem CICS na každé z následujících platforem:

- AIX AIX
- Windows Windows

Každý soubor načtení přepínače obsahuje funkci, která vrací ukazatel na strukturu přepínače XA používanou pro dynamickou registraci MQRMIXASwitchDynamic. Úplný název cesty každého zaváděcího souboru přepínače viz Tabulka 5 na stránce 26 .

Tabulka 5. Soubory načtení přepínače

Platforma	Soubor načtení přepínače
AIX AIX Linux Linux	*MQ_INSTALLATION_PATH*/lib/amqczsc
Windows	*MQ_INSTALLATION_PATH*\bin\mqcc4swi.dll [1]

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

Zde je příklad definice prostředku XAD pro systémy Windows :

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

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

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

- Do oblasti CICS můžete přidat pouze jednu definici prostředku XAD pro IBM MQ . To znamená, že k určité oblasti může být přidružen pouze jeden správce front a všechny aplikace CICS spuštěné v dané oblasti se mohou připojit pouze k tomuto správci front. Chcete-li spustit aplikace systému CICS , které se připojují k jinému správci front, musíte spustit aplikace v jiné oblasti.
- Každý aplikační server v oblasti volá xa_open během inicializace a spouští kanál MQI pro správce front přidruženého k dané oblasti. To znamená, že správce front musí být spuštěn před spuštěním aplikačního serveru, jinak volání xa_open selže. Všechny aplikace IBM MQ MQI client , které byly později zpracovány aplikačním serverem, používají stejný kanál MQI.
- Při spuštění kanálu MQI a při neexistenci uživatelské procedury zabezpečení na straně klienta kanálu je ID uživatele, které směřuje z klientského systému do agenta MCA pro připojení k serveru, `cics` . Za určitých okolností správce front používá toto ID uživatele pro kontrolu oprávnění, když se agent MCA připojení serveru následně pokusí o přístup k prostředkům správce front jménem klientské aplikace. Pokud se toto ID uživatele používá pro kontroly oprávnění, musíte se ujistit, že má oprávnění pro přístup ke všem prostředkům, ke kterým potřebuje přístup.

  Informace o tom, kdy správce front používá toto ID uživatele pro kontroly oprávnění, naleznete v tématu Zabezpečení.
- Uživatelské procedury ukončení úlohy CICS , které jsou dodávány pro použití v klientských systémech IBM MQ , jsou uvedeny v části Tabulka 6 na stránce 27 . Tyto uživatelské procedury nakonfigurujete stejným způsobem, jakým nakonfigurujete odpovídající uživatelské procedury pro systémy serveru IBM MQ . Tyto informace viz Povolení CICS uživatelských procedur.

Tabulka 6. Ukončení úlohy CICS

Platforma	Zdroj	Knihovna
AIX AIX Linux Linux	amqzscgx.c	amqczscg (česky)
Windows Windows systémy	amqzscgn.c	mqcc1415.dll

Konfigurace rozšířeného transakčního klienta pro produkt Tuxedo

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

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

- V sekci GROUPS souboru Tuxedo UBBCONFIG pro aplikaci použijte parametr **OPENINFO** k uvedení řetězce xa_open. Příklad, jak to provést, viz ukázkový soubor UBBCONFIG, který je dodáván pro použití s ukázkovými programy Tuxedo.

  AIX Na následujících platformách je název souboru `ubbstxcx.cfg`:

– AIX

Windows, název souboru je `ubbstxcn.cfg`.

- V položce pro správce front v tabulce správce prostředků Tuxedo zadejte název struktury přepínače XA a úplný název cesty ke knihovně, která strukturu obsahuje:
  – AIX V systémech AIXzadejte hodnotu `udataobj/RM`.
  – Windows V systému Windowszadejte hodnotu `udataobj\rm`.

  Příklad, jak to provést pro každou platformu, viz Ukázky TUXEDO. Tuxedo podporuje dynamickou registraci správce prostředků, takže můžete použít buď MQRMIXASwitch, nebo MQRMIXASwitchDynamic.

Windows Microsoft Transakční server

Před použitím serveru Microsoft Transaction Server (MTS) jako správce transakcí není vyžadována žádná další konfigurace. Nicméně, tam jsou některé body na vědomí.

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

- Aplikace MTS vždy spustí kanál MQI, když se připojí ke správci front serveru. Modul MTS ve své roli správce transakcí poté ke komunikaci se správcem front používá stejný kanál MQI.
- Po selhání musí být MTS schopen obnovit všechny nedokončené jednotky práce. Za tímto účelem musí být modul MTS schopen komunikovat se všemi správci front, kteří se v době selhání podíleli na nedokončené transakci.

  Když se aplikace MTS připojí ke správci front serveru a spustí kanál MQI, rozšířený transakční klient v případě potřeby extrahuje z parametrů volání MQCONN nebo MQCONNX dostatečné informace, aby umožnil restartování kanálu po selhání. Rozšířený transakční klient předává informace MTS a MTS zaznamenává informace do svého protokolu.

  Pokud aplikace MTS zadá volání MQCONN, jedná se pouze o název správce front. Pokud aplikace MTS zadá volání MQCONNX a poskytne strukturu definice kanálu MQCD, informace zahrnují také název kanálu MQI, síťovou adresu správce front serveru a komunikační protokol kanálu.

  V situaci zotavení předá modul MTS tyto informace zpět rozšířenému transakčnímu klientovi a rozšířený transakční klient je použije k restartování kanálu MQI.

  Pokud potřebujete změnit jakékoli informace o konfiguraci, ujistěte se, že všechny nedokončené jednotky práce byly vyřešeny před provedením změn. Případně se ujistěte, že změny konfigurace neovlivňují schopnost rozšířeného transakčního klienta restartovat kanál MQI pomocí informací zaznamenaných MTS. Zde jsou příklady takových změn konfigurace:
  – Změna hodnoty proměnné prostředí MQSERVER
  – Změna položek v tabulce CCDT (Client Channel Definition Table)
  – Odstranění definice kanálu připojení serveru
- Při použití rozšířeného transakčního klienta s MTS mějte na paměti následující podmínky:
  – V rámci jednoho podprocesu může být klientská aplikace v daném okamžiku připojena pouze k jednomu správci front.
  – Každý podproces klientské aplikace 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, jednu pro každý konec připojení s použitím stejného názvu kanálu a kompatibilních typů kanálů. V tomto případě jsou typy kanálů *server-connection* a *client-connection*.

Kanály definované uživatelem

Pokud server nedefinuje kanály automaticky, existují dva způsoby, jak vytvořit definice kanálů a poskytnout aplikaci IBM MQ na počítači se systémem IBM MQ MQI client přístup ke kanálu.

Tyto dvě metody jsou podrobně popsány:

1. Vytvořte jednu definici kanálu v klientu IBM MQ a druhou na serveru.

   Toto platí pro libovolnou kombinaci platforem IBM MQ MQI client a serverů. Použijte jej při zahájení práce v systému nebo při testování nastavení.

   Podrobnosti o použití této metody naleznete v části “Vytvoření definic připojení serveru a připojení klienta na různých platformách” na stránce 34 .
2. Vytvořte obě definice kanálů na počítači serveru.

   Tuto metodu použijte, když nastavujete více kanálů a počítače se systémem IBM MQ MQI client současně.

   Podrobnosti o použití této metody naleznete v části “Vytvoření definic připojení serveru a připojení klienta na serveru” na stránce 40 .

Automaticky definované kanály

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

Pokud je od klienta obdržen příchozí požadavek na připojení a příslušná definice připojení serveru nebyla v daném správci front nalezena, produkt IBM MQ vytvoří definici automaticky a přidá ji do správce front. Automatická definice je založena na definici výchozího kanálu připojení serveru SYSTEM.AUTO.SVRCONN. Automatickou definici definic připojení serveru povolíte aktualizací objektu správce front pomocí příkazu ALTER QMGR s parametrem CHAD (nebo pomocí příkazu PCF Změnit správce front s parametrem ChannelAutoDef).

Související pojmy

“Funkce řízení kanálu” na stránce 218
Funkce řízení kanálu poskytuje prostředky pro definování, monitorování a řízení kanálů.

ALW Vytváření a používání kanálů AMQP

Při instalaci podpory produktu IBM MQ pro komponentu služby AMQP do instalace produktu IBM MQ můžete spustit příkaz IBM MQ MQSC (**runmqsc**) a definovat, pozměnit, odstranit, spustit a zastavit kanál. Můžete také zobrazit stav kanálu.

Než začnete

Tato úloha předpokládá, že jste nainstalovali kanál AMQP. To provedete výběrem komponenty AMQP SERVICE při instalaci produktu IBM MQ. Chcete-li získat další informace, postupujte podle odkazu pro vaši platformu a pak vyhledejte řádek tabulky pro "AMQP Service":

- AIX IBM MQ komponenty pro systémy AIX
- Linux IBM MQ komponenty rpm pro systémy Linux
- Linux IBM MQ Debian komponenty pro systémy Linux Ubuntu
- Windows IBM MQ funkce pro systémy Windows

Poznámka: Viz Restartování služby IBM MQ pro AMQP , kde naleznete příklad komponenty SERVICE a další informace, pokud vaše služba AMQP přestane pracovat správně.

Tato úloha také předpokládá, že máte existujícího správce front.

Chcete-li vytvořit testovací připojení ke správci front, můžete použít všechny klienty AMQP, kteří implementují protokol OASIS AMQP 1.0 , například klienty MQ Light a Apache Qpid, jako např. Apache Qpid Proton a Apache Qpid JMS.

V 9.3.0 V systému IBM MQ 9.3.0můžete použít pouze výchozí kanál SYSTEM.DEF.AMQPtestuje připojení MQ Light ke správci front. Následující postup používá výchozí kanál.

Tato úloha je založena na klientovi MQ Light Node.js . Kroky týkající se správce front IBM MQ jsou však pro každého klienta stejné.

Poznámka: Kanály AMQP nepodporují služby AMQP definované uživatelem. Kanály MQP podporují pouze výchozí systém SYSTEM.AMQP.SERVICE . Pro každého správce front lze definovat pouze jednu instanci této služby.

Postup

1. Spusťte **runmqsc** z adresáře *mqinstall*/bin/ :

   ```
   runmqsc QMNAME
   ```

2. (Nezbytné pouze v případě, že váš správce front je IBM MQ 9.0.4 nebo starší.) Zkontrolujte, zda je funkce AMQP nainstalována a zda správně funguje.

   Pomocí příkazu **START SERVICE** spusťte službu IBM MQ , která řídí prostředí JVM:

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

   Poznámka: Ze IBM MQ 9.1 SYSTÉMU SYSTEM.AMQP.SERVICE má atribut **CONTROL** nastaven na *QMGR*. To způsobí automatické spuštění služby při spuštění správce front. Nastavením atributu **CONTROL** na hodnotu *MANUAL*můžete zabránit spuštění služby při spuštění správce front.

   Při spuštění správce front se automaticky spustí služba AMQP a kanál AMQP, jsou-li definovány.

3. Nastavte ID uživatele MCAUSER .

   Když se klient AMQP připojí ke kanálu, kanál určuje ID uživatele MCAUSER , které se používá pro připojení ke správci front. Výchozí hodnota MCAUSER je prázdná. Aby se mohli klienti AMQP připojit ke správci front, musíte zadat hodnotu MCAUSER , která musí být platným uživatelem produktu IBM MQ , který je oprávněn publikovat a odebírat témata IBM MQ .

   Poznámka: Windows V systému Windowspřed IBM MQ 9.2.0je nastavení ID uživatele MCAUSER podporováno pouze pro ID uživatelů s délkou nejvýše 12 znaků. Od verze IBM MQ 9.2.0 již neplatí limit délky max. 12 znaků.

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

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

   b) Pomocí následujících dvou příkazů **setmqaut** autorizujte ID uživatele MCAUSER pro publikování a odběr témat:

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

   a

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

   Pokud je kanál spuštěn v době, kdy je ID uživatele MCAUSER přidáno nebo změněno, musíte kanál zastavit a restartovat.

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

4. Pomocí příkazu **START CHANNEL** spusťte výchozí SYSTEM.DEF.AMQP :

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

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

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

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

6. Změňte výchozí port.

Výchozí port pro připojení AMQP 1.0 je 5672. Pokud již používáte port 5672, což je možné, pokud jste dříve nainstalovali produkt MQ Light, musíte změnit port, který používá váš kanál AMQP. Pomocí příkazu **ALTER CHANNEL** změňte port:

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

7. Pokud nechcete blokovat nebo filtrovat připojení ke kanálu AMQP pomocí pravidel ověřování kanálu (CHLAUTH), zakažte ověřování kanálu ve správci front následujícím způsobem:

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

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

Případně nakonfigurujte pravidla ověřování kanálu správce front tak, aby umožňovala specifická připojení ke kanálu AMQP.

8. Volitelné: Chcete-li u kanálu povolit šifrování SSL/TLS s použitím konfigurovaného úložiště klíčů pro správce front, musíte nastavit atribut SSLCIPH pro kanál na odpovídající specifikaci šifrování. Standardně je specifikace šifry prázdná, což znamená, že šifrování SSL/TLS se na kanálu nepoužívá. Pomocí příkazu **ALTER CHANNEL** nastavte specifikaci šifry. Příklad:

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

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

- Ve výchozím nastavení je certifikát v úložišti klíčů správce front s popiskem odpovídajícím atributu **CERTLABL** správce front název používaný šifrováním SSL/TLS pro daný kanál. Můžete vybrat jiný certifikát nastavením **CERTLABL**. Pomocí příkazu **ALTER CHANNEL** zadejte popisek pro požadovaný certifikát:

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

- Můžete nastavit kanál tak, aby vyžadoval certifikát od připojení klienta SSL/TLS. Nastavením atributu **SSLCAUTH** můžete vybrat, zda se požaduje certifikát z připojení klienta SSL/TLS. Použijte příkaz **ALTER CHANNEL** k nastavení, zda je požadován certifikát z připojení klienta SSL/TLS. Příklad:

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

- Pokud nastavíte atribut **SSLCAUTH** na hodnotu REQUIRED, lze zkontrolovat rozlišující název (DN) certifikátu od klienta. Chcete-li zkontrolovat rozlišující název certifikátu z klienta, nastavte atribut

SSLPEER . Pomocí příkazu **ALTER CHANNEL** zkontrolujte rozlišující název certifikátu z klienta. Příklad:

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

Alternativně můžete také použít záznamy ověření kanálu k povolení nebo blokování připojení, protože tato metoda nabízí větší granularitu v porovnání s použitím atributu **SSLPEER** . Další informace o nastavení **SSLPEER** a použití záznamů ověření kanálu jako alternativy viz SSL Peer.

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

```
npm install mqlight
```

10. Přejděte do adresáře `node_modules/mqlight/samples` a spusťte ukázkovou aplikaci příjemce:
    - Pokud používáte výchozí číslo portu, můžete spustit ukázkovou aplikaci příjemce:

      ```
      node recv.js
      ```

    - Pokud jste konfigurovali kanál AMQP tak, aby používal jiné číslo portu, můžete spustit ukázkovou přijímací aplikaci s parametrem pro zadání nového čísla portu:

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

    Úspěšné připojení k výchozímu kanálu zobrazí následující zprávu:

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

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

    Poznámka: Pokud neuvedete parametr `-i` , automaticky se vygeneruje `client-id` .
11. V novém příkazovém okně přejděte do adresáře `node_modules/mqlight/samples` a spusťte ukázkovou aplikaci odesilatele spuštěním následujícího příkazu:

    ```
    node send.js
    ```

    V příkazovém okně pro aplikaci příjemce se zobrazí zpráva `Ahoj světe` .
12. Ukázku **AMQSSUB** IBM MQ použijte k přijetí ukázkové zprávy MQ Light .

    V systémech Linux a Windowslze ukázku nalézt v následujících umístěních:
    - Linux *mqinstall*`/samp/bin` adresář na Linux.
    - Windows *mqinstall*`/Tools\c\Samples\Bin` adresář na Windows.

    a) Spusťte ukázku spuštěním následujícího příkazu:

    ```
    amqssub public QM-name.
    ```

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

    ```
    node send.js
    ```

13. Pomocí příkazu **DEFINE CHANNEL** vytvořte další kanály AMQP:

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

Když definujete kanál, musí být ručně spuštěn pomocí příkazu **START CHANNEL** :

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

Chcete-li zkontrolovat, zda kanál běží správně, můžete spustit ukázkovou přijímací aplikaci a určit port nového kanálu:

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

Jak pokračovat dále

K zobrazení připojení IBM MQ , zastavení kanálu a odstranění kanálu můžete použít následující příkazy:

DISPLAY CONN(*) TYPE(*CONN*) WHERE (*CHANNEL EQ SYSTEM.DEF.AMQP*)
Zobrazuje připojení IBM MQ , které kanál AMQP vytvořil ve správci front.

DISPLAY CHSTATUS(*) CHLTYPE(*AMQP*) CLIENTID(*) ALL
Zobrazí seznam klientů AMQP připojených k uvedenému kanálu.

STOP CHANNEL (*MY.AMQP.CHANNEL*)
Zastaví kanál AMQP a zavře port, na kterém naslouchá.

DELETE CHANNEL (*MY.AMQP.CHANNEL*)
Odstraní všechny kanály, které jste vytvořili.

Poznámka: Neodstraňujte výchozí kanál SYSTEM.DEF.AMQP.

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

- Pomocí produktu **runmqsc**zobrazte atributy správce front a zkontrolujte `AMQPCAP(YES)`.
- Pomocí PCF použijte příkaz **MQCMD_INQUIRE_Q_MGR** a potvrďte hodnotu `MQIA_AMQP_CAPABILITY`.

Související úlohy
Vývoj klientských aplikací AMQP
Zabezpečení klientů AMQP
Související odkazy
strmqm

ALW Odebrání kanálu AMQP ze správců front

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

Postup

1. Zastavte správce front.
2. Odeberte podporu IBM MQ pro rozhraní API komponenty služby AMQP:
   - AIX V produktu AIX spusťte následující příkaz:

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

   - Linux V systému Linuxodeberte RPM AMQP. Pokud jste před instalací znovu zabalili RPM, zadejte název nově zabaleného RPM.

     ```
     rpm -e MQSeriesAMQP
     ```

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

3. Restartujte správce front.

Související úlohy

Vývoj klientských aplikací AMQP

Zabezpečení klientů AMQP

ALW Soubory protokolu kanálu AMQP

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

Výchozí datový adresář v systému Windows je `C:\ProgramData\IBM\MQ`.

Výchozí datový adresář v systému Linux je `/var/mqm`.

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

- `amqp.stdout`, zapsaná do složky `qmgrs/`*`QM-name`* .
- `amqp.stderr`, zapsaná do složky `qmgrs/`*`QM-name`* .
- `amqp_*.log` , zapsaná do složky `qmgrs/`*`QM-name`*`/errors` .

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

Všechny soubory FDC jsou vytvořeny jako soubory `AMQP*.FDC` , které jsou zapsány do složky *`data-directory`*`/errors` .

Některé konfigurační soubory jsou zapsány do adresáře `qmgrs/`*`QM-name`*`/amqp` . Není třeba upravovat žádné soubory v tomto adresáři.

Související pojmy

Protokoly chyb na AIX, Linux, and Windows

Související úlohy

Vývoj klientských aplikací AMQP

Zabezpečení klientů AMQP

Vytvoření definic připojení serveru a připojení klienta na různých platformách

Každou definici kanálu můžete vytvořit na počítači, na který se vztahuje. Existují však omezení týkající se způsobu vytváření definic kanálů v klientském počítači.

Informace o této úloze

Na všech platformách můžete k definování kanálu připojení serveru v počítači serveru použít příkazy MQSC (IBM MQ Script), PCF (Programmable Command Format) nebo IBM MQ Explorer .

z/OS Na systému z/OS můžete také použít ovládací a ovládací panely.

IBM i V systému IBM i můžete také použít rozhraní panelu.

Protože příkazy MQSC nejsou k dispozici na počítači, kde byl produkt IBM MQ nainstalován pouze jako IBM MQ MQI client , musíte použít různé způsoby definování kanálu připojení klienta na klientském počítači.

Následující aspekty platí pro **runmqsc**:

- Můžete zadat parametr **-c** a volitelně také parametr **-u** pro připojení **runmqsc** jako klienta ke správci front, kterého chcete spravovat.
- Pokud použijete parametr **-u** k zadání ID uživatele, budete vyzváni k zadání odpovídajícího hesla.

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

Procedura

- Chcete-li na serveru definovat kanál připojení serveru, postupujte podle části "Definování kanálu připojení serveru na serveru" na stránce 35.
- Chcete-li vytvořit kanál připojení klienta v systému IBM MQ MQI client pomocí proměnné prostředí **MQSERVER** , viz "Vytvoření kanálu připojení klienta v systému IBM MQ MQI client pomocí MQSERVER" na stránce 36.
- Chcete-li vytvořit kanál připojení klienta v systému IBM MQ MQI clientpomocí struktury MQCNO ve volání MQCONNX, viz "Vytvoření kanálu připojení klienta v produktu IBM MQ MQI client pomocí MQCNO" na stránce 39.

Definování kanálu připojení serveru na serveru

V případě potřeby spusťte prostředí MQSC a poté 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 spuštěném na serveru.
3. Chcete-li povolit přístup pro příchozí připojení ke správci front, použijte následující příkaz:

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

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

   Příchozí připojení můžete identifikovat pomocí několika různých atributů. Příklad používá adresu IP. Mezi alternativní atributy patří ID uživatele klienta a rozlišující název předmětu TLS. Další informace naleznete v tématu Záznamy ověření kanálu .

Vytvoření kanálu připojení klienta v systému IBM MQ MQI client pomocí MQSERVER

Kanál připojení klienta na pracovní stanici klienta můžete definovat pomocí proměnné prostředí **MQSERVER** .

Informace o této úloze

Pomocí proměnné prostředí **MQSERVER** můžete určit jednoduchou definici kanálu připojení klienta. Je to jednoduché v tom smyslu, že pomocí této metody můžete zadat pouze několik atributů kanálu.

Pokud k definování kanálu mezi počítačem se systémem IBM MQ MQI client a počítačem se serverem použijete proměnnou prostředí **MQSERVER** , jedná se o jediný kanál, který je k dispozici pro vaši aplikaci, a na tabulku CCDT (Client Channel Definition Table) se neodkazuje.

Pokud požadavek MQCONN nebo MQCONNX uvádí jiného správce front, než ke kterému je připojen modul listener, nebo pokud není rozpoznán parametr **MQSERVER** *TransportType* , požadavek MQCONN nebo MQCONNX selže s návratovým kódem MQRC_Q_MGR_NAME_ERROR.

Linux AIX V systému AIX and Linuxmůžete definovat **MQSERVER** jako jeden z následujících příkladů:

```
export MQSERVER=CHANNEL1/TCP/'9.20.4.56(2002)'
export MQSERVER=CHANNEL1/LU62/BOX99
```

Všechny požadavky MQCONN nebo MQCONNX se poté pokusí použít kanál, který jste definovali, pokud se na strukturu MQCD neodkazuje ze struktury MQCNO dodané do MQCONNX. V takovém případě má kanál určený strukturou MQCD přednost před jakýmkoli kanálem určeným proměnnou prostředí **MQSERVER** .

Proměnná prostředí **MQSERVER** má přednost před jakoukoli definicí kanálu klienta, na kterou ukazují proměnné prostředí **MQCHLLIB** a **MQCHLTAB** .

Procedura

- V závislosti na vaší platformě použijte jeden z následujících příkazů k určení definice kanálu s produktem **MQSERVER**.
  - Windows V systému Windowszadejte jednoduchou definici kanálu následujícím způsobem:

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

    Příklad:

    ```
    export  MQSERVER='SYSTEM.DEF.SVRCONN/TCP/AMACHINE.ACOMPANY.COM(1414)'
    ```

  - Linux AIX V systému AIX and Linuxzadejte jednoduchou definici kanálu následujícím způsobem:

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

    Příklad:

    ```
    SET  MQSERVER=SYSTEM.DEF.SVRCONN/TCP/AMACHINE.ACOMPANY.COM(1414)
    ```

  - IBM i V systému IBM izadejte jednoduchou definici kanálu následujícím způsobem:

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

Příklad:

```
ADDENVVAR ENVVAR(MQSERVER) VALUE('SYSTEM.DEF.SVRCONN/TCP/AMACHINE.ACOMPANY.COM(1414)')
```

Notes:

- *ChannelName* musí mít stejný název, jaký je definován na serveru. Nemůže obsahovat dopředné lomítko (/), protože tento znak se používá k oddělení názvu kanálu, typu transportu a názvu připojení. Je-li k definování kanálu klienta použita proměnná prostředí **MQSERVER** , použije se maximální délka zprávy (**MAXMSGL**) 100 MB. Proto je maximální velikost zprávy platná pro kanál hodnotou určenou v kanálu SVRCONN na serveru.
- Typ *TransportType* může být LU62, TCP, NETBIOS, SPX, v závislosti na vaší klientské platformě IBM MQ .
- Linux AIX V systému AIX and Linux *TransportType* rozlišuje velikost písmen a musí být velká písmena. Volání MQCONN nebo MQCONNX vrátí hodnotu 2058, pokud není rozpoznán typ transportu.
- *ConnectionName* je název serveru, jak je definován pro komunikační protokol (*TransportType*). Musí to být úplný název sítě, například AMACHINE.ACOMPANY.COM(1414).
- *ConnectionName* může být seznam názvů připojení oddělených čárkami. Názvy připojení v seznamu se používají podobným způsobem jako více připojení v tabulce připojení klienta. Seznam názvů připojení lze použít jako alternativu ke skupinám správců front k určení více připojení, která má klient vyzkoušet. Pokud konfigurujete správce front s více instancemi, můžete použít seznam názvů připojení k určení různých instancí správce front.

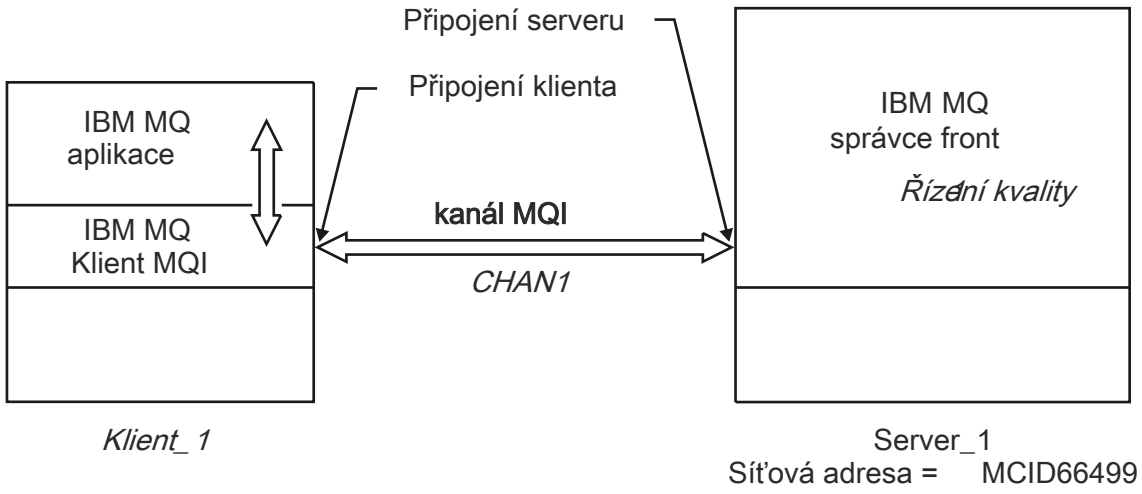
- Chcete-li zrušit soubor **MQSERVER** a vrátit se do tabulky definic kanálů klienta, na kterou ukazují **MQCHLLIB** a **MQCHLTAB**, zadejte následující příkaz:
  - Linux AIX V systému AIX and Linux:

    ```
    unset MQSERVER
    ```

  - Windows V systému Windows:

    ```
    SET MQSERVER=
    ```

Příklad



Obrázek 1. Příklad jednoduché definice kanálu

Chcete-li vytvořit jednoduchou definici kanálu zobrazenou v souboru Obrázek 1 na stránce 37, použijte následující příkazy:

- Linux AIX V systému AIX and Linux:

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

- Windows V systému Windows:

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

Poznámka: Informace o tom, jak změnit číslo portu TCP/IP, viz “Změna výchozího portu TCP/IP” na stránce 38.

Některé další příklady jednoduchých definic kanálů jsou následující:

- Windows V systému Windows:

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

- Linux AIX V systému AIX and Linux:

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

  kde B0X99 je logická jednotka 6.2 ConnectionName.

- IBM i V systému IBM i:

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

V systému IBM MQ MQI clientse všechny požadavky **MQCONN** nebo **MQCONNX** poté pokusí použít kanál, který jste definovali, pokud není kanál přepsán ve struktuře MQCD odkazované ze struktury MQCNO dodané do produktu **MQCONNX**.

Související úlohy

“Použití proměnných prostředí IBM MQ” na stránce 61
Pomocí příkazů můžete zobrazit aktuální nastavení nebo resetovat hodnoty proměnných prostředí IBM MQ .

“Vytvoření kanálu připojení klienta v produktu IBM MQ MQI client pomocí MQCNO” na stránce 39
Kanál připojení klienta na pracovní stanici klienta můžete definovat pomocí struktury MQCNO ve volání MQCONNX.

Změna výchozího portu TCP/IP

Ve výchozím nastavení pro protokol TCP/IP produkt IBM MQ předpokládá, že kanál bude připojen k portu 1414. V případě potřeby můžete změnit výchozí hodnotu.

Informace o této úloze

Číslo portu můžete změnit pomocí jedné z následujících tří voleb:

- Pomocí proměnné prostředí **MQSERVER** .
- Změnou souboru `mqclient.ini` .
- Přidáním IBM MQ do souboru služeb.

Procedura

- Chcete-li změnit číslo portu pomocí proměnné prostředí **MQSERVER** , přidejte číslo portu v závorkách jako poslední část *ConnectionName*, například:
  - Linux AIX V systému AIX and Linux:

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

  - Windows V systému Windows:

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

- Chcete-li změnit číslo portu pomocí souboru `mq.ini` , přidejte číslo portu k názvu protokolu, například:

  ```
  TCP:
  port=2001
  ```

- Chcete-li změnit číslo portu přidáním IBM MQ do souboru služeb, postupujte podle pokynů v části “Použití modulu listener TCP/IP v systému AIX and Linux” na stránce 259.

Windows *Změna výchozího soketu SPX*

Ve výchozím nastavení pro SPX produkt IBM MQ předpokládá, že kanál bude připojen k soketu 5E86. V případě potřeby můžete změnit výchozí hodnotu.

Informace o této úloze

Číslo portu můžete změnit pomocí jedné z následujících voleb:

- Pomocí proměnné prostředí **MQSERVER** .

  Pro připojení SPX zadejte ConnectionName a soket ve formátu `network.node(socket)`. Pokud jsou klient a server IBM MQ ve stejné síti, síť nemusí být uvedena. Pokud používáte výchozí soket, soket nemusí být uveden.
- Změnou sekce SPX souboru `mqclient.ini` file.Changing souboru `qm.ini` .

Procedura

- Chcete-li změnit číslo portu pro připojení SPX pomocí proměnné prostředí **MQSERVER** , zadejte *ConnectionName* a soket ve tvaru `network.node(socket)` , jak ukazuje následující příklad:

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

  Poznámka: Pokud se klient a server IBM MQ nacházejí ve stejné síti, nemusíte zadávat síť. Používáte-li výchozí soket, nemusíte jej zadávat.
- Chcete-li změnit číslo portu pomocí souboru `qm.ini` , přidejte číslo portu k názvu protokolu, například:

  ```
  SPX:
  socket=5E87
  ```

Vytvoření kanálu připojení klienta v produktu IBM MQ MQI client pomocí MQCNO

Kanál připojení klienta na pracovní stanici klienta můžete definovat pomocí struktury MQCNO ve volání MQCONNX.

Informace o této úloze

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

Tímto způsobem může klientská aplikace určit atributy **ChannelName**, **TransportType**a **ConnectionName** kanálu za běhu, což umožní klientské aplikaci připojit se k více správcům front serveru současně.

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

Klientská aplikace může také určit atributy kanálu, například **MaxMsgLength** a **SecurityExit**. Zadání těchto atributů umožní klientské aplikaci zadat hodnoty pro atributy, které nejsou výchozími hodnotami, a umožní volání programů uživatelské procedury kanálu na klientském konci kanálu MQI.

Pokud kanál používá protokol TLS (Transport Layer Security), může klientská aplikace také poskytnout informace týkající se protokolu TLS ve struktuře MQCD. Další informace týkající se TLS lze poskytnout ve struktuře voleb konfigurace TLS, MQSCO, na kterou také odkazuje struktura MQCNO ve volání **MQCONNX** .

Další informace o strukturách MQCNO, MQCD a MQSCO viz MQCNO, MQCDa MQSCO.

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

Související úlohy

"Vytvoření kanálu připojení klienta v systému IBM MQ MQI client pomocí MQSERVER" na stránce 36
Kanál připojení klienta na pracovní stanici klienta můžete definovat pomocí proměnné prostředí **MQSERVER** .

Vytvoření definic připojení serveru a připojení klienta na serveru

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

Informace o této úloze

Nejprve definujte kanál připojení serveru a poté definujte kanál připojení klienta:

- Na všech platformách můžete definovat kanál připojení serveru v počítači serveru pomocí příkazů MQSC (IBM MQ Script), příkazů PCF (Programmable Command Format).
- Windows Linux V systémech Linux a Windowsmůžete také použít IBM MQ Explorer.
- z/OS V systému z/OSmůžete také použít ovládací a ovládací panely.
- IBM i V systému IBM i můžete také použít rozhraní panelu.

Definice kanálů připojení klienta vytvořené na serveru jsou zpřístupněny klientům pomocí tabulky CCDT (Client Channel Definition Table).

Postup

1. Chcete-li definovat kanál připojení serveru, postupujte podle části "Definování kanálu připojení serveru na serveru" na stránce 53.
2. Chcete-li definovat kanál připojení klienta, viz "Definování kanálu připojení klienta na serveru" na stránce 54.

Související úlohy

"Konfigurace binárního formátu CCDT" na stránce 41
Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformě Multiplatforms se při vytvoření správce front automaticky vytvoří binární tabulka CCDT obsahující výchozí nastavení. Příkaz **runmqsc** se používá k aktualizaci binární tabulky CCDT.

“Definování kanálu připojení serveru na serveru” na stránce 53
Vytvořte definici kanálu připojení serveru pro správce front.

“Definování kanálu připojení klienta na serveru” na stránce 54
Po definování kanálu připojení serveru můžete definovat odpovídající kanál připojení klienta.

“Přístup k definicím kanálů připojení klienta” na stránce 55
Tabulku CCDT (Client Channel Definition Table) můžete zpřístupnit klientským aplikacím zkopírováním nebo sdílením této tabulky a poté zadat její umístění a název v klientském počítači. Tabulku CCDT (Client Channel Definition Table) můžete také vyhledat prostřednictvím URL.

Konfigurace tabulek definic kanálů klienta

Tabulka CCDT (Client Channel Definition Table) definuje kanály připojení klienta a jejich atributy. Klienti čtou tento soubor a zjišťují, ke kterým správcům front se mají připojit. Soubor CCDT může být buď ve formátu JSON, nebo v binárním formátu.

Informace o této úloze

Správce front nečte soubor CCDT. Používá se pouze k poskytování definic kanálů a ověřovacích informací klientům.

Před IBM MQ 9.2.0je tabulka CCDT k dispozici pouze v binárním formátu. V produktu IBM MQ 9.2.0můžete také vytvořit CCDT ve formátu JSON (JavaScript Object Notation).

CCDT binárního formátu se vytvoří automaticky při vytvoření správce front. Definice kanálů klienta uložené v této tabulce aktualizujete pouze pomocí příkazu **runmqsc** .

Formát JSON CCDT je prostý textový soubor s příponou .json. Tuto tabulku vytvoříte a aktualizujete ručně, což je méně omezující než použití příkazu **runmqsc** .

z/OS Klienti produktu z/OS JMS běžící na aplikačním serveru používají k odkazování na podrobnosti připojení vzdáleného správce front tabulky CCDT. V systému IBM MQ for z/OS 9.1umožňuje produkt IBM MQ Advanced for z/OS Value Unit Edition klientům JMS vzdálené připojení ke správcům front v jiných oblastech LPAR systému z/OS . Proto mohou tito klienti také používat tabulky CCDT.

Chcete-li pomoci konfigurovat tabulky CCD tak, aby spolupracovaly s klienty, vyberte si z následujících úloh:

Procedura

- “Konfigurace binárního formátu CCDT” na stránce 41
- “Konfigurace formátu JSON CCDT” na stránce 44
- “Umístění pro tabulky CCDT” na stránce 51
- “Přístup URL k tabulce CCDT” na stránce 52

Související pojmy
Klient MQI: Tabulka CCDT (Client Channel Definition Table)
Související úlohy
“Konfigurace jednotného klastru” na stránce 400
Jednotné klastry umožňují navrhovat aplikace pro škálování a dostupnost a mohou se připojovat k libovolným správcům front v rámci tohoto jednotného klastru.

Konfigurace binárního formátu CCDT

Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformě Multiplatforms se při vytvoření správce front automaticky vytvoří binární tabulka CCDT obsahující výchozí nastavení. Příkaz **runmqsc** se používá k aktualizaci binární tabulky CCDT.

Než začnete

Z produktu IBM MQ 9.1.2můžete také vytvořit CCDT ve formátu JSON JavaScript Object Notation (JSON) a použití tohoto alternativního formátu má některé výhody oproti použití binárního CCDT. Viz téma “Konfigurace formátu JSON CCDT” na stránce 44.

Klienti na všech platformách mohou zobrazovat a používat tabulky CCD. Binární CCDT však lze vytvořit a upravit pouze v adresáři IBM MQ for Multiplatforms.

Informace o této úloze

Multi V systému Multiplatforms:

- Binární tabulka CCDT se vytvoří automaticky v adresáři `@ipcc` v datovém adresáři pro správce front.
- Kromě automatického vytváření je binární tabulka CCDT přidružená ke správci front synchronizována s definicemi objektů. Při definování, změně nebo odstranění objektu kanálu klienta dojde k aktualizaci definice objektu správce front i položky v tabulce CCDT v rámci stejné operace.

  Notes:

  – Návrh souboru IBM MQ CCDT spočívá v tom, že soubor CCDT je zmenšen až poté, co jsou všechny kanály připojení klienta definované uživatelem skutečně definovány. Je-li kanál připojení klienta odstraněn, je pouze označen jako odstraněný v souboru CCDT, ale není fyzicky odstraněn.

  – Chcete-li vynutit zmenšení souboru CCDT po odstranění jednoho nebo více kanálů připojení klienta, zadejte následující příkaz:

  ```
  rcrmqobj -m QM80 -t clchltab
  ```

- Pomocí příkazu **runmqsc** můžete změnit umístění a obsah binární tabulky CCDT.

Klienti na všech platformách mohou zobrazit a používat binární CCDT.

Procedura

- Multi

  Vytvořte výchozí binární CCDT.

  V systému Multiplatformsje při vytváření správce front vytvořena výchozí binární tabulka CCDT s názvem `AMQCLCHL.TAB` .

  Standardně se jedná o AMQCLCHL.TAB je umístěn v následujícím adresáři na serveru:

  – IBM i V systému IBM iv integrovaném systému souborů:

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

  – Linux AIX Na systémech AIX and Linux:

  /prefix/qmgrs/*QUEUEMANAGERNAME*/@ipcc

  Název adresáře, na který odkazuje *QUEUEMANAGERNAME* , rozlišuje velká a malá písmena na systémech AIX and Linux . Název adresáře se nemusí shodovat s názvem správce front, pokud v něm název správce front obsahuje speciální znaky.

  – Windows V systému Windows:

  MQ_INSTALLATION_PATH\data\qmgrs*QUEUEMANAGERNAME*\@ipcc

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

Je však možné, že jste zvolili použití jiného adresáře pro data správce front. Při použití příkazu **crtmqm** můžete zadat parametr **-md** *DataPath* . Pokud tak učiníte, soubor AMQCLCHL.TAB se nachází v adresáři @ipcc zadané cesty *DataPath* .

- Vyhledejte tabulky CCDT:
  - Na klientském počítači
  - V umístění sdíleném více než jedním klientem
  - Na serveru jako sdílený soubor

  Viz "Umístění pro tabulky CCDT" na stránce 51.

  a) Vytvořte binární CCDT přímo na klientském počítači.
    - Použijte příkaz runmqsc s parametrem **-n** .
    - Tabulka CCDT je vytvořena v umístění označeném jako **MQCHLLIB**a s názvem souboru označeným jako **MQCHLTAB**, což je standardně AMQCLCHL.TAB .
    - **Důležité:** Zadáte-li parametr **-n** , nesmíte zadat žádný jiný parametr.

  b) Změňte umístění.

  Cestu k tabulce CCDT můžete změnit nastavením **MQCHLLIB**. Mějte na paměti, že pokud máte na jednom serveru více správců front, sdílejí stejné umístění CCDT.
- Přístup k tabulce CCDT

  K tabulce CCDT můžete přistupovat:
  - Vzdáleně ze souboru, ftp nebo http URLdefinováním proměnné prostředí **MQCCDTURL** .
  - Lokálně nastavením proměnných prostředí **MQCHLLIB** a **MQCHLTAB** .
  - Lokálně definováním atributů **ChannelDefinitionDirectory** a **ChannelDefinitionFile** sekce CHANNELS v konfiguračním souboru klienta.

  Různé příklady viz "Umístění pro tabulky CCDT" na stránce 51 .
- Zobrazte nebo upravte obsah tabulky CCDT.

  Obsah tabulky CCDT můžete zobrazit pomocí příkazu **runmqsc** :

  1. Nastavte proměnné prostředí na Přístup k tabulce CCDT
  2. Spusťte příkaz runmqsc -n
  3. Spusťte příkaz DISPLAY CHANNEL (*), například

  Multi V systému Multiplatformsmůžete také upravit binární obsah tabulky CCDT pomocí příkazu **runmqsc** . Každá položka tabulky CCDT představuje připojení klienta ke specifickému správci front. Nová položka se přidá, když definujete kanál připojení klienta pomocí příkazu **DEFINE CHANNEL** , a položka se aktualizuje, když změníte kanály připojení klienta pomocí příkazu **ALTER CHANNEL** . Další příklady použití příkazu viz **runmqsc** .
- Poskytněte klientům ověřovací informace pro kontrolu odvolání certifikátu TLS.

  a) Definujte seznam názvů obsahující objekty ověřovacích informací.

  b) Nastavte atribut správce front **SSLCRLNL** na název seznamu názvů.

Související pojmy

Práce se zrušenými certifikáty

Související úlohy

"Konfigurace formátu JSON CCDT" na stránce 44

Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. K vytvoření a aktualizaci JSON JavaScript Object Notation (JSON) se používá textový editor. CCDT.

Konfigurace formátu JSON CCDT

Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. K vytvoření a aktualizaci JSON JavaScript Object Notation (JSON) se používá textový editor. CCDT.

Než začnete

Multi Používáte-li produkt IBM MQ for Multiplatforms, můžete místo toho použít binární CCDT, které se vytvoří automaticky při vytvoření správce front. Viz téma “Konfigurace binárního formátu CCDT” na stránce 41.

Informace o této úloze

Název souboru schématu CCDT pro formát JSON je:

Linux

```
/opt/mqm/lib/ccdt_schema.json
```

Windows

```
C:\Program Files\IBM\MQ\bin\ccdt_schema.json
```

Neexistuje žádná výchozí tabulka JSON CCDT a produkt IBM MQ nedodává žádné nástroje pro vytvoření nebo úpravu tabulky CCDT ve formátu JSON. Nicméně při ručním vývoji tabulky JSON CCDT máte více voleb konfigurace, než když používáte příkaz **runmqsc** pro práci s binární tabulkou CCDT:

- Nemusíte používat produkt IBM MQ for Multiplatforms k vytvoření a úpravě souboru JSON CCDT.
- Pomocí formátu JSON můžete definovat duplicitní definice kanálu se stejným názvem. Při implementaci produktu IBM MQ v cloudu jej můžete použít k tomu, aby byla vaše implementace rozšiřitelná a vysoce dostupná.
- Soubor JSON je čitelný pro člověka, což může zjednodušit konfiguraci správce front.
- Formát prostého textového souboru lze integrovat s:
  - Nástroje pro správu verzí pro sledování historie tabulky CCDT
  - Automatizační nástroje v nepřetržitém dodání
- K údržbě souboru CCDT nepotřebujete žádné specializované nástroje.
- Soubor je menší.
- Tento formát poskytuje zpětnou a dopřednou kompatibilitu.

Notes:

1. Standard JSON považuje duplicitní klíče za platné, avšak syntaktický analyzátor JSON vezme při přiřazování atributů pouze hodnotu posledního čtení duplicitních klíčů. Proto při definování duplicitních kanálů musí být každý kanál prvkem hodnoty pole, která je přiřazena ke klíči 'channel'.
2. Tabulky CCD JSON nepodporují ukládání umístění serveru LDAP (Lightweight Directory Access Protocol) pro seznamy odvolaných certifikátů (CRL) a informace o umístění odpovídacího modulu OCSP (Online Certificate Status Protocol).

Tabulka 7. Požadavky na kódování podle platformy

Platforma	Kódování klienta JMS	Kódování klienta jazyka C
IBM i IBM i	ASCII	EBCDIC
ALW AIX, Linux, and Windows	ASCII	ASCII
z/OS z/OS	Buď ASCII, nebo EBCDIC	Nelze použít

Upozornění: Když poskytnete jakoukoli definici kanálu prostřednictvím tabulky JSON CCDT (včetně *řídké* definice, která nezahrnuje všechny atributy), je úplná definice kanálu sestavena se všemi definovanými atributy s použitím výchozích hodnot pro vše, co není uvedeno ve formátu JSON.

Proto musíte zadat specifické hodnoty pro každý atribut, pro který nechcete výchozí hodnotu.

Procedura

- Vytvořit tabulky CCDT JSON
  a) Vytvořte prostý textový soubor s příponou `.json` s generickým textovým editorem.
  b) Definujte tabulky CCDT.

  Další informace jsou uvedeny v tématech “Příklady JSON CCDT” na stránce 48 a “Atributy kanálu podporované tabulkou JSON CCDT” na stránce 46.
- Vyhledejte tabulky CCDT:
  - Na klientském počítači
  - V umístění sdíleném více než jedním klientem
  - Na serveru jako sdílený soubor

  Viz “Umístění pro tabulky CCDT” na stránce 51.
- Ověření tabulky CCDT JSON

  Ověřte CCDT proti schématu pomocí linteru JSON.

  Informace o tom, jak vytvořit soubor CCDT se dvěma kanály a ověřit jeho fungování, naleznete v tématu Jak ověřit soubor JSON produktu IBM MQ CCDT vůči schématu .

  Schéma CCDT je součástí balíků produktu a klienta:

  - Linux AIX Na systémech AIX and Linux:

    `$MQ_INSTALLATION_PATH/lib` a `/lib` v balících produktu a klienta.
  - Windows V systému Windows:

    `%MQ_INSTALLATION_PATH%\bin` a `\bin` v balících produktu a klienta.

  Notes:

  - Ukazatele JSON jsou k dispozici online.
  - Schéma definuje povinné atributy s klíčem '`required`'.
  - Schéma definuje datové typy atributů s klíčem '`type`'.
- Přístup k tabulce CCDT

  K tabulce CCDT můžete přistupovat:

  - Vzdáleně ze souboru, ftp nebo http URLdefinováním proměnné prostředí **MQCCDTURL** .
  - Lokálně nastavením proměnných prostředí **MQCHLLIB** a **MQCHLTAB** .
  - Lokálně definováním atributů **ChannelDefinitionDirectory** a **ChannelDefinitionFile** sekce CHANNELS v konfiguračním souboru klienta.

  Různé příklady viz “Umístění pro tabulky CCDT” na stránce 51 .
- Zobrazit nebo upravit obsah tabulky CCDT

  Každá položka tabulky CCDT představuje připojení klienta ke specifickému správci front. Obsah tabulky CCDT můžete zobrazit nebo upravit pomocí textového editoru.

  Chcete-li zobrazit pouze tabulky CCDT, můžete to provést také pomocí příkazu **runmqsc** :

1. Nastavte proměnné prostředí, abyste získali přístup k tabulce CCDT, jak je popsáno v předchozím kroku.
2. Spusťte příkaz `runmqsc -n` . Další informace viz runmqsc.
3. Spusťte příkaz **`DISPLAY CHANNEL`** . Spusťte například příkaz `DISPLAY CHANNEL(*)`.

Související pojmy

Práce se zrušenými certifikáty

Související úlohy

“Konfigurace binárního formátu CCDT” na stránce 41

Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformě Multiplatforms se při vytvoření správce front automaticky vytvoří binární tabulka CCDT obsahující výchozí nastavení. Příkaz **`runmqsc`** se používá k aktualizaci binární tabulky CCDT.

“Konfigurace jednotného klastru” na stránce 400

Jednotné klastry umožňují navrhovat aplikace pro škálování a dostupnost a mohou se připojovat k libovolným správcům front v rámci tohoto jednotného klastru.

Atributy kanálu podporované tabulkou JSON CCDT

Seznam atributů kanálu připojení klienta podporovaných tabulkou JSON CCDT. Tento seznam je podmnožinou atributů podporovaných binární tabulkou CCDT.

Mapování atributu

Tyto atributy jsou vloženy do následujícího objektu kanálu:

```
{ "channel": [ {$CHANNEL_1_KEY_VALUE_LIST },..., {$CHANNEL_N_KEY_VALUE_LIST } ] }
```

kde `$CHANNEL_X_KEY_VALUE_LIST` je čárkami oddělený seznam atributů uvedených v následující tabulce.

Základní příklady použití viz “Příklady JSON CCDT” na stránce 48 .

Schéma JSON se dodává v adresáři `/opt/mqm/lib/ccdt_schema.json`. Chcete-li zjistit, jaké hodnoty jsou platné pro každý z atributů, podívejte se na schéma JSON.

Následující tabulka vypisuje objekt JSON, klíč a datový typ spolu s odpovídající definicí atributu binárního kanálu.

Upozornění: Povinné atributy jsou kanál **`name`** a kanál **`type`**. Pokud také definujete **`portRange`**, atributy *low* a *high* jsou také povinné.

Objekt JSON	Klíč JSON	Datový typ JSON	Definice binárního atributu
kanál (pole)	Název	String	CHANNEL
kanál (pole)	typ	String	CHLTYPE
channel.clientConnection	queueManager	String	QMNAME
channel.clientConnection.connection (pole)	hostitel	String	CONNAME
channel.clientConnection.connection	Port	INT	CONNAME
channel.compression.header (pole)	záhlaví	String	COMPHDR
channel.compression.message (pole)	zpráva	String	COMPMSG
channel.connectionManagement	afinita	String	AFFINITY
channel.connectionManagement	clientWeight	INT	CLNTWGHT

Objekt JSON	Klíč JSON	Datový typ JSON	Definice binárního atributu
channel.connectionManagement	defaultReconnect	String	DEFRECON
channel.connectionManagement	disconnectInterval	INT	DISCINT
channel.connectionManagement	heartInterval	INT	HBINT
channel.connectionManagement	KeepAliveInterval	INT	KAINT
channel.connectionManagement	sharingConversations	INT	SHARECNV
channel.connectionManagement.localAddress (pole)	hostitel	String	LOCLADDR
channel.connectionManagement.localAddress (pole)	Port	INT	LOCLADDR
channel.connectionManagement.localAddress.portRange	vysoká	INT	LOCLADDR
channel.connectionManagement.localAddress.portRange	nízká	INT	LOCLADDR
channel.exits.receive (pole)	Název	String	RCVEXIT
channel.exits.receive (pole)	userData	String	RCVDATA
channel.exits.security	Název	String	SCYEXIT
channel.exits.security	userData	String	SCYDATA
channel.exits.send (pole)	Název	String	SENDEXIT
channel.exits.send (pole)	userData	String	SENDDATA
channel.general	description	String	DESCR
channel.general	maximumMessageDélka	INT	MAXMSGL
channel.timestamps	změněno	String	ALTDATE a ALTTIME
channel.transmissionSecurity	certificateLabel	String	CERTLABL
channel.transmissionSecurity	Název certificatePeer	String	SSLPEER
channel.transmissionSecurity	cipherSpecification	String	SSLCIPH

Notes:

- `channel.connectionManagement.localAddress` lze definovat jako jednu z následujících kombinací kláves:
  - Hostitel a port
  - hostitel a portRange
  - Port
  - portRange
- Klíč JSON `channel.timestamps altered` je volitelný a není-li definován, hodnota je standardně nastavena na čas poslední úpravy souboru JSON CCDT. Pokud je však prostředí nakonfigurováno pro načtení tabulky CCDT z URL, výchozí hodnota je čas, kdy byl soubor naposledy stažen.
- `channel.clientConnection.connection` musí obsahovat klíče hostitele i portu.

- Změněný klíč je jediný řetězec, který zapouzdřuje atributy ALTDATE a ALTTIME.
- Typ přenosu může být pouze TCP, proto nejsou ve schématu definovány následující atributy:
  - **TRPTYPE**
  - **USERID**
  - **PASSWORD**
  - **MODENAME**
  - **TPNAME**

Související odkazy
Atributy kanálu pro typy kanálů

Příklady JSON CCDT
Příklady uvedené v tomto tématu použijte jako základ vašich požadavků.

Otevřete generický textový editor a zkopírujte jeden z následujících příkladů:

- “Definovat jednoduché připojení klienta” na stránce 48
- “Definovat jeden kanál a jednoho správce front pomocí protokolu TLS” na stránce 48
- “Definovat jeden kanál a jednoho správce front, který nepoužívá protokol TLS” na stránce 49
- “Definovat dva kanály se stejným názvem” na stránce 49
- “Úplný seznam definic atributů kanálu CCDT pro kanál připojení klienta” na stránce 50

Definovat jednoduché připojení klienta

```
{
  "channel":
  [
    {
      "general":
      {
        "description": "a channel"
      },
      "name": "channel",
      "clientConnection":
      {
        "connection":
        [
          {
            "host": "localhost",
            "port": 1414
          }
        ],
        "queueManager": "QM1"
      },
      "type": "clientConnection"
    }
  ]
}
```

Definovat jeden kanál a jednoho správce front pomocí protokolu TLS

```
{
  "channel": [
    {
      "name": "SSL.SVRCONN",
      "clientConnection": {
        "connection": [
          {
            "host": "aztlan1.fyre.ibm.com",
            "port": 1419
          }
        ],
        "queueManager": "QM92TLS"
      },
      "transmissionSecurity":
```

```
      {
        "cipherSpecification": "TLS_AES_128_GCM_SHA256",
        "certificateLabel": "ibmwebspheremqadministrator",
      },
      "type": "clientConnection"
    }
  ]
}
```

Definovat jeden kanál a jednoho správce front, který nepoužívá protokol TLS

```
{
  "channel": [
    {
      "name": "SYSTEM.DEF.SVRCONN",
      "clientConnection": {
        "connection": [
          {
            "host": "aztlan1.fyre.ibm.com",
            "port": 1414
          }
        ],
        "queueManager": "QM92"
      },
      "type": "clientConnection"
    }
  ]
}
```

Definovat dva kanály se stejným názvem

Každý kanál se připojuje ke dvěma odlišným správcům front:

```
{
  "channel":
  [
    {
      "general":
      {
        "description": "First channel"
      },
      "name": "channel",
      "clientConnection":
      {
        "connection":
        [
          {
            "host": "localhost",
            "port": 1414
          }
        ],
        "queueManager": "QM1"
      },
      "type": "clientConnection"
    },
    {
      "general":
      {
        "description": "Second channel"
      },
      "name": "channel",
      "clientConnection":
      {
        "connection":
        [
          {
            "host": "localhost",
            "port": 1415
          }
        ],
        "queueManager": "QM2"
      },
      "type": "clientConnection"
    }
```

```
  ]
}
```

Úplný seznam definic atributů kanálu CCDT pro kanál připojení klienta

```
{
  "channel":
  [
    {
      "compression":
      {
        "header": [ "system" ],
        "message": [ "zlibfast" ]
      },
      "connectionManagement":
      {
        "sharingConversations": 10,
        "clientWeight": 1,
        "affinity": "none",
        "defaultReconnect": "yes",
        "heartbeatInterval": 600,
        "keepAliveInterval": -1,
        "localAddress":
        [
          {
            "portRange":
            {
              "low": 2020,
              "high": 3030
            }
          }
        ]
      },
      "exits":
      {
        "receive":
        [
          {
          "name": "",
          "userData": ""
          }
        ],
        "security":
        {
          "name": "",
          "userData": ""
        },
        "send":
        [
           {
             "name": "",
             "userData": ""
           }
        ]
      },
      "general":
      {
        "description": "First channel",
        "maximumMessageLength": 4194304
      },
      "name": "the_channel",
      "clientConnection":
      {
        "connection":
        [
          {
            "host": "localhost",
            "port": 1414
          }
        ],
        "queueManager": "QM1"
      },
      "timestamps":
      {
        "altered": "2018-12-04T15:37:22.000Z"
      },
      "transmissionSecurity":
      {
        "cipherSpecification": "",
```

```
        "certificateLabel": "",
        "certificatePeerName": ""
      },
      "type": "clientConnection"
    }
  ]
}
```

Související odkazy

Atributy kanálu pro typy kanálů

Atributy kanálu v abecedním pořadí

Umístění pro tabulky CCDT

Produkt IBM MQ podporuje načítání tabulky CCDT ze souboru, FTP nebo HTTP URL. CCDT můžete zpřístupnit pro klienta jako sdílený soubor, zatímco zůstane umístěn na serveru. Případně můžete CCDT distribuovat buď zkopírováním tabulky CCDT do jednotlivých klientských počítačů, nebo zkopírováním tabulky CCDT do umístění sdíleného více než jedním klientem.

Pokud ke kopírování souboru používáte protokol FTP, použijte volbu `bin` k nastavení binárního režimu; nepoužívejte výchozí režim `ASCII` . Ať už se rozhodnete zpřístupnit CCDT jakoukoli metodou, umístění musí být bezpečné, aby se zabránilo neoprávněným změnám v kanálech.

Jak hostovat soubor CCDT na serveru

Z produktu IBM MQ 9.0může být tabulka CCDT hostována v centrálním umístění, které je přístupné prostřednictvím URL, což odstraňuje potřebu individuální aktualizace tabulky CCDT pro každého implementovaného klienta. Produkt IBM MQ 9.0 přidal schopnost nativních (C/C + +, COBOL a RPG) a nespravovaných aplikací .NET stáhnout CCDT z URL, ať už se jedná o lokální soubor, prostředek FTP nebo HTTP .

Výchozí chování klientů IBM MQ při ukládání do mezipaměti spočívá v tom, že soubor CCDT je stažen pouze v případě, že se čas úpravy souboru liší od času posledního načtení. Stejně jako u většiny voleb konfigurace klienta existuje řada způsobů, jak lze zadat umístění URL :

- **CCDTUrlPtr** a **CCDTUrlOffset** prostřednictvím struktury MQCNO předávané do volání MQCONNX MQI
- **MQCCDTURL** proměnná prostředí
- **ChannelDefinitionDirectory** atribut v sekci Kanály `mqclient.ini`

Jsou podporovány ověřené i neověřené adresy URL. Několik příkladů:

```
export MQCCDTURL=ftp://myuser:password@myhost.sample.com//var/mqm/qmgrs/QMGR/@ipcc/AMQCLCHL.TAB
```

```
export MQCCDTURL=http://myhost.sample.com/var/mqm/qmgrs/QMGR/@ipcc/AMQCLCHL.TAB
```

Chcete-li tuto podporu používat s FTP nebo HTTP, musíte i nadále hostovat soubor CCDT na serveru, ale s podporou přidanou na adrese IBM MQ 9.0mohou všechny klientské aplikace automaticky vybírat změny v definicích kanálů bez nutnosti ručního odesílání aktualizací nebo připojení síťového systému souborů na každého klienta. Další informace viz téma “Přístup URL k tabulce CCDT” na stránce 52.

Jak určit umístění tabulky CCDT na klientovi

V klientském systému můžete určit umístění tabulky CCDT následujícími způsoby:

- Pomocí proměnných prostředí **MQCHLLIB** uveďte adresář, kde je tabulka umístěna, a **MQCHLTAB** uveďte název souboru tabulky.
- Použití konfiguračního souboru klienta. V sekci CHANNELS použijte atribut **ChannelDefinitionDirectory** k uvedení adresáře, kde se nachází tabulka, a atribut **ChannelDefinitionFile** k uvedení názvu souboru.
- Poskytnutím URL (soubor, FTP nebo HTTP) pro CCDT, která je hostována v centrálním umístění, jak bylo popsáno výše.

Je-li umístění zadáno jak v konfiguračním souboru klienta, tak pomocí proměnných prostředí, mají proměnné prostředí prioritu. Pomocí této funkce můžete určit standardní umístění v konfiguračním souboru klienta a v případě potřeby ji přepsat pomocí proměnných prostředí.

Pokud k zadání umístění tabulky CCDT používáte URL , pořadí, v jakém má aplikace nativního klienta přednost při hledání definice kanálu klienta, je popsáno v tématu “Přístup URL k tabulce CCDT” na stránce 52.

Přístup URL k tabulce CCDT

Tabulku CCDT (Client Channel Definition Table) můžete hostovat v centrálním umístění, ke kterému lze přistupovat prostřednictvím URL, což eliminuje potřebu individuální aktualizace tabulky CCDT pro každého implementovaného klienta.

V produktu IBM MQ 9.0lze tabulku definic kanálů klienta vyhledat prostřednictvím URL jedním z následujících způsobů:

- Programováním pomocí MQCNO
- Pomocí proměnných prostředí

  Upozornění: Volbu proměnné prostředí můžete použít k zadání URL pouze pro nativní programy, které se připojují jako klienti, tj. aplikace C, COBOL nebo C + +. Proměnné prostředí nemají žádný vliv na aplikace Java, JMS nebo spravované .NET .

  Produkt IBM MQ podporuje načítání tabulky CCDT ze souboru, ftp nebo http URL.
- Pomocí sekce Kanály souboru `mqclient.ini` .

Proměnná prostředí **MQCCDTURL** vám umožňuje poskytnout soubor, ftp nebo http URL jako jedinou hodnotu, ze které lze získat tabulku definic kanálů klienta.

Můžete také použít cestu k adresáři určenou proměnnou prostředí **MQCHLLIB** (nebo cestu určenou atributem **ChannelDefinitionDirectory** v souboru “Sekce kanálů konfiguračního souboru klienta” na stránce 171) k vyhledání souboru CCDT, buď prostřednictvím souboru, ftp, nebo http URL, kromě existujícího adresáře lokálního systému souborů, tj. `/var/mqm`). Všimněte si, že hodnota **MQCHLLIB** je adresářový kmen a pracuje v kombinaci s **MQCHLTAB** pro odvození úplné URL.

Základní ověření u připojení je podporováno prostřednictvím pověření, která jsou zakódována v URL:

Ověřená připojení

```
export MQCHLLIB=ftp://myuser:password@myhost.sample.com/var/mqm/qmgrs/QMGR/@ipcc
export MQCHLLIB=http://myuser:password@myhost.sample.com/var/mqm/qmgrs/QMGR/@ipcc
```

Neověřená připojení

```
export MQCHLLIB=ftp://myhost.sample.com/var/mqm/qmgrs/QMGR/@ipcc
export MQCHLLIB=http://myhost.sample.com/var/mqm/qmgrs/QMGR/@ipcc
export MQCHLLIB=file:///var/mqm/qmgrs/QMGR/@ipcc
```

Poznámka: Chcete-li používat ověřená připojení, musíte, stejně jako v případě produktu JMS, zadat jméno uživatele a heslo zakódované v URL.

Pořadí přednosti pro nativní klientskou aplikaci při hledání definice kanálu klienta je nyní:

1. MQCD poskytovaný produktem **ClientConnOffset** a **ClientConnPtr** v MQCNO.
2. URL poskytovaná **CCDTUrlOffset** a **CCDTUrlPtr** v MQCNO.
3. *MQSERVER* proměnná prostředí.
4. Je-li definován soubor `mqclient.ini` a sekce Kanály obsahuje atribut **ServerConnectionParms** , použije se kanál, který definuje. Další informace naleznete v tématu “IBM MQ MQI client konfigurační soubor mqclient.ini” na stránce 155 a “Sekce kanálů konfiguračního souboru klienta” na stránce 171.
5. **MQCCDTURL** proměnná prostředí.
6. **MQCHLLIB** a **MQCHLTAB** proměnná prostředí.

7. **ChannelDefinitionDirectory** a **ChannelDefinitionFile** v souboru “Sekce kanálů konfiguračního souboru klienta” na stránce 171.

Důležité: Přístup k souboru CCDT pomocí URL vždy otevře kopii souboru jen pro čtení, a to i při použití protokolu `file://` .

Pokus o otevření souboru CCDT pro přístup pro zápis, například při použití příkazu **DEFINE CHANNEL** MQSC z klienta, vrátí chybovou zprávu označující, že soubor nelze otevřít pro přístup pro zápis.

Je však možné číst definice kanálu a ověřovacích informací pomocí **runmqsc**.

Související úlohy

“Přístup k definicím kanálů připojení klienta” na stránce 55
Tabulku CCDT (Client Channel Definition Table) můžete zpřístupnit klientským aplikacím zkopírováním nebo sdílením této tabulky a poté zadat její umístění a název v klientském počítači. Tabulku CCDT (Client Channel Definition Table) můžete také vyhledat prostřednictvím URL.

“Konfigurace binárního formátu CCDT” na stránce 41
Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformě Multiplatforms se při vytvoření správce front automaticky vytvoří binární tabulka CCDT obsahující výchozí nastavení. Příkaz **runmqsc** se používá k aktualizaci binární tabulky CCDT.

Použití tabulky CCDT s IBM MQ classes for JMS

Související odkazy

CCDTURL

MQCNO-Volby připojení

XMSC_WMQ_CCDTURL

Windows Kanály připojení klienta v adresáři Active Directory

V systémech Windows , které podporují Active Directory, produkt IBM MQ publikuje kanály připojení klienta ve službě Active Directory , aby poskytoval dynamickou vazbu klient-server.

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

1. MQCONNX Datová struktura MQCD
2. **MQSERVER** proměnná prostředí
3. Soubor definice kanálu klienta
4. Active Directory

Toto pořadí znamená, že žádné aktuální aplikace nejsou ovlivněny žádnou změnou. Tyto položky v adresáři Active Directory si můžete představit jako záznamy v souboru definice kanálu klienta a klient IBM MQ je zpracuje stejným způsobem. Chcete-li konfigurovat a spravovat podporu pro publikování definic kanálů připojení klienta ve službě Active Directory, použijte příkaz `setmqscp` , jak je popsáno v tématu setmqscp.

Definování kanálu připojení serveru na serveru

Vytvořte definici kanálu připojení serveru pro správce front.

Postup

1. V počítači serveru definujte kanál s vybraným názvem a typem kanálu *server-connection*.
   Příklad:

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

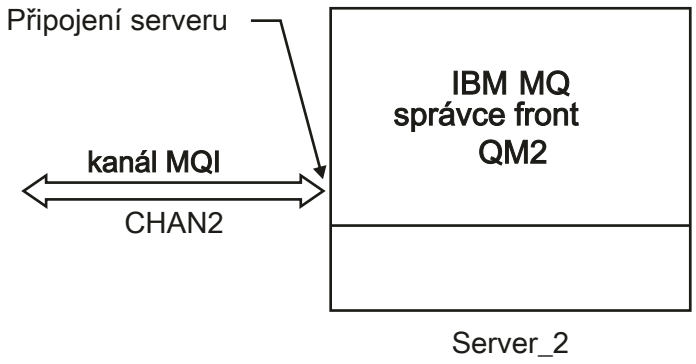
2. Chcete-li povolit přístup pro příchozí připojení ke správci front, použijte následující příkaz:

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

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

Příchozí připojení můžete identifikovat pomocí několika různých atributů. Příklad používá adresu IP. Mezi alternativní atributy patří ID uživatele klienta a rozlišující název předmětu TLS. Další informace naleznete v tématu Záznamy ověření kanálu .

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



Obrázek 2. Definování kanálu připojení serveru

Související úlohy

“Definování kanálu připojení klienta na serveru” na stránce 54
Po definování kanálu připojení serveru můžete definovat odpovídající kanál připojení klienta.

Definování kanálu připojení klienta na serveru

Po definování kanálu připojení serveru můžete definovat odpovídající kanál připojení klienta.

Než začnete

Definujte kanál připojení serveru. Další informace viz téma “Definování kanálu připojení serveru na serveru” na stránce 53.

Postup

1. Definujte kanál se stejným názvem jako kanál připojení serveru, ale s typem kanálu *připojení klienta*. Musíte uvést název připojení (CONNAME). V případě TCP/IP je název připojení síťová adresa nebo název hostitele počítače serveru. Doporučuje se také zadat název správce front (QMNAME), ke kterému se má aplikace IBM MQ spuštěná v prostředí klienta připojovat. 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. Chcete-li povolit přístup pro příchozí připojení ke správci front, použijte následující příkaz:

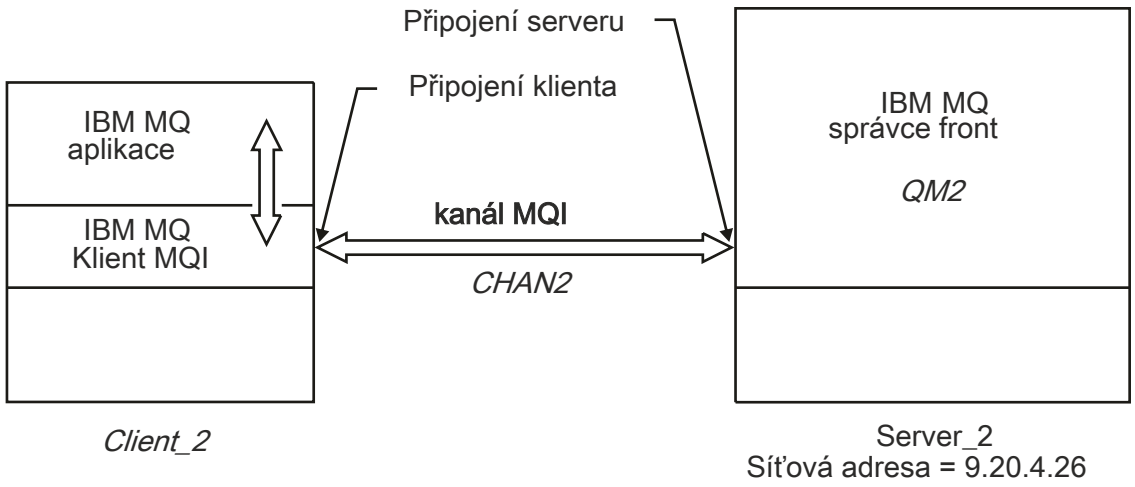
```
SET CHLAUTH(CHAN2) TYPE(ADDRESSMAP) ADDRESS('IP-address') MCAUSER('userid')
```

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

Příchozí připojení můžete identifikovat pomocí několika různých atributů. Příklad používá adresu IP. Mezi alternativní atributy patří ID uživatele klienta a rozlišující název předmětu TLS. Další informace naleznete v tématu Záznamy ověření kanálu .

Výsledky

Multi V systému Multiplatformsje tato definice kanálu uložena v souboru s názvem 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 odpovídající informace o tom, jak jsou definice kanálů připojení klienta uloženy v systému z/OS, viz “Konfigurace binárního formátu CCDT” na stránce 41.



Obrázek 3. Definování kanálu připojení klienta

Související odkazy
DEFINE CHANNEL (definovat nový kanál)
SET CHLAUTH (vytvořit nebo upravit záznam ověření kanálu)

Přístup k definicím kanálů připojení klienta

Tabulku CCDT (Client Channel Definition Table) můžete zpřístupnit klientským aplikacím zkopírováním nebo sdílením této tabulky a poté zadat její umístění a název v klientském počítači. Tabulku CCDT (Client Channel Definition Table) můžete také vyhledat prostřednictvím URL.

Než začnete

Tato úloha předpokládá, že jste v tabulce CCDT definovali kanály připojení klienta, které potřebujete. Viz “Konfigurace tabulek definic kanálů klienta” na stránce 41.

Informace o této úloze

Aby mohla klientská aplikace používat tabulku CCDT (Client Channel Definition Table), je třeba ji zpřístupnit a určit její umístění a název. Existuje několik způsobů, jak to udělat:

- CCDT můžete zkopírovat do klientského počítače.
- CCDT můžete zkopírovat do umístění sdíleného více než jedním klientem.
- CCDT můžete zpřístupnit pro klienta jako sdílený soubor, zatímco zůstane umístěn na serveru.

IBM MQ nativní (C/C + +, COBOL a RPG) a nespravované aplikace .NET mohou stáhnout CCDT hostované v centrálním umístění z URL, ať už se jedná o lokální soubor, prostředek ftp nebo http.

Postup

1. Zpřístupněte tabulky CCDT klientským aplikacím jedním z následujících způsobů:
   a) Volitelné: Zkopírujte CCDT do klientského počítače.
   b) Volitelné: Zkopírujte tabulky CCDT do umístění sdíleného více než jedním klientem.
   c) Volitelné: Ponechte tabulky CCDT na serveru, ale zpřístupněte je pro sdílení klientem.
   d) Volitelné: Definujte lokální soubor, ftp nebo http URL pro CCDT hostované v centrálním umístění, aby nativní (C/C + +, COBOL a RPG) a nespravované aplikace .NET mohly stáhnout CCDT z této URL.

   Bez ohledu na umístění, které zvolíte pro CCDT, musí být umístění zabezpečené, aby se zabránilo neoprávněným změnám v kanálech.
2. Na klientovi zadejte umístění a název souboru obsahujícího CCDT jedním ze tří způsobů:
   a) Volitelné: Použijte sekci CHANNELS konfiguračního souboru klienta. Další informace viz téma “Sekce kanálů konfiguračního souboru klienta” na stránce 171.
   b) Volitelné: Použijte proměnné prostředí **MQCHLLIB** a **MQCHLTAB**.

      Proměnné prostředí můžete nastavit například zadáním následujícího příkazu:

      - Linux AIX Na systémech AIX and Linux:

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

      - IBM i Na systémech IBM i:

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

      kde *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .
   c) Volitelné: Pouze v systému Windows použijte řídicí příkaz **setmqscp** k publikování definic kanálů připojení klienta ve službě Active Directory.
   d) Zadejte umístění centrálně hostované tabulky CCDT prostřednictvím URL, buď pomocí programování pomocí MQCNO, pomocí proměnných prostředí, nebo pomocí sekcí souboru `mqclient.ini` . Další informace viz “Umístění pro tabulky CCDT” na stránce 51 a “Přístup URL k tabulce CCDT” na stránce 52.

   Je-li nastavena proměnná prostředí **MQSERVER** , klient IBM MQ použije definici kanálu připojení klienta určenou parametrem **MQSERVER** namísto definic v tabulce definic kanálů klienta.

Související úlohy

“Konfigurace binárního formátu CCDT” na stránce 41
Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformě Multiplatforms se při vytvoření správce front automaticky vytvoří binární tabulka CCDT obsahující výchozí nastavení. Příkaz **runmqsc** se používá k aktualizaci binární tabulky CCDT.

Související odkazy

Klient MQI: Tabulka CCDT (Client Channel Definition Table)

ALW Programy uživatelské procedury kanálu pro kanály MQI

Pro prostředí IBM MQ MQI client v systému AIX, Linux, and Windowsjsou k dispozici tři typy uživatelské procedury kanálu.

Patří mezi ně:

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

Tyto uživatelské procedury jsou k dispozici na straně klienta i na straně serveru kanálu. Uživatelské procedury nejsou pro vaši aplikaci k dispozici, pokud používáte proměnnou prostředí MQSERVER. Uživatelské procedury kanálu jsou vysvětleny v tématu Programy uživatelských procedur kanálu pro kanály systému zpráv.

Odeslání a příjem ukončí práci společně. Existuje několik možných způsobů, jak je můžete použít:

- Rozdělení a opětovné sestavení zprávy
- Komprimace a dekomprimace dat ve zprávě (tato funkce je poskytována jako součást produktu IBM MQ, ale možná budete chtít použít jinou techniku komprese).
- Šifrování a dešifrování uživatelských dat (tato funkce je poskytována jako součást produktu IBM MQ, ale možná budete chtít použít jinou techniku šifrování).
- Žurnálování každé odeslané a přijaté zprávy

Uživatelskou proceduru zabezpečení můžete použít k zajištění správné identifikace klienta a serveru IBM MQ a k řízení přístupu.

Pokud uživatelské procedury pro odesílání nebo příjem na straně připojení serveru instance kanálu potřebují provést volání MQI pro připojení, ke kterému jsou přidruženy, použijí manipulátor připojení uvedený v poli MQCXP Hconn . Je třeba si uvědomit, že uživatelské procedury pro odesílání a příjem připojení klienta nemohou provádět volání MQI.

Související pojmy

“Uživatelské procedury zabezpečení pro připojení klienta” na stránce 58
Můžete použít uživatelské procedury zabezpečení, abyste ověřili, že partner na druhém konci kanálu je pravý. Při použití uživatelské procedury zabezpečení pro připojení klienta platí zvláštní pokyny.

Uživatelské procedury, uživatelské procedury rozhraní API a instalovatelné služby IBM MQ

Související úlohy

Rozšíření prostředků správce front

Související odkazy

“Cesta k východům” na stránce 57
Výchozí cesta pro umístění uživatelských procedur kanálu je definována v konfiguračním souboru klienta. Uživatelské procedury kanálu jsou načteny při inicializaci kanálu.

“Identifikace volání API v programu uživatelské procedury pro odeslání nebo příjem” na stránce 59
Používáte-li kanály MQI pro klienty, bajt 10 vyrovnávací paměti agenta identifikuje volání rozhraní API, které se používá při volání uživatelské procedury pro odeslání nebo příjem. To je užitečné pro identifikaci toho, které toky kanálů zahrnují uživatelská data a mohou vyžadovat zpracování, například šifrování nebo digitální podepisování.

ALW Cesta k východům

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

Na systémech AIX, Linux, and Windows se konfigurační soubor klienta přidá do vašeho systému během instalace produktu IBM MQ MQI client. Výchozí cesta pro umístění uživatelských procedur kanálu na klientovi je definována v tomto souboru pomocí sekce:

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

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

Při inicializaci kanálu se po volání MQCONN nebo MQCONNX prohledává konfigurační soubor klienta. Sekce ClientExitPath je přečtena a všechny uživatelské procedury kanálu, které jsou uvedeny v definici kanálu, jsou načteny.

ALW Uživatelské procedury zabezpečení pro připojení klienta

Můžete použít uživatelské procedury zabezpečení, abyste ověřili, že partner na druhém konci kanálu je pravý. Při použití uživatelské procedury zabezpečení pro připojení klienta platí zvláštní pokyny.

Obrázek 4 na stránce 59 ilustruje použití uživatelských procedur zabezpečení v připojení klienta pomocí správce oprávnění k objektu IBM MQ k ověření uživatele.

Pole SecurityParmsPtr nebo SecurityParmsOffset ve struktuře MQCNO je nastaveno klientem a existují uživatelské procedury zabezpečení na obou koncích kanálu. Po ukončení normální výměny zpráv zabezpečení a po připravení kanálu ke spuštění je struktura MQCSP předána uživatelské proceduře zabezpečení klienta. Uživatelská procedura může přistupovat ke struktuře MQCSP pomocí pole SecurityParms ve struktuře MQCXP. Typ ukončení je nastaven na MQXR_SEC_PARMS. Uživatelská procedura zabezpečení může změnit pověření ve struktuře MQCSP nebo je ponechat beze změny.

Data vrácená z uživatelské procedury se pak odešlou na konec připojení serveru kanálu. Struktura MQCSP je znovu sestavena na konci připojení serveru kanálu a předána uživatelské proceduře zabezpečení připojení serveru. Uživatelská procedura může přistupovat ke struktuře MQCSP pomocí pole SecurityParms ve struktuře MQCXP. Uživatelská procedura zabezpečení přijme a zpracuje tato data. Toto zpracování obvykle slouží k vrácení všech změn pověření ve struktuře MQCSP pomocí uživatelské procedury klienta, které jsou poté použity k autorizaci připojení správce front. Na výslednou strukturu MQCSP se odkazuje pomocí SecurityParmsPtr ve struktuře MQCNO v systému správce front.

Adresa paměti vrácená s polem SecurityParms struktury MQCXP musí zůstat adresovatelná a nezměněná, dokud nebude MQXR_TERM. Uživatelská procedura nesmí zneplatnit nebo uvolnit paměť zpět do systému před zavoláním uživatelské procedury pro MQXR_TERM.

Je-li ve struktuře MQCNO nastaveno pole SecurityParmsPtr nebo SecurityParmsOffset a existuje-li uživatelská procedura zabezpečení pouze na jednom konci kanálu, uživatelská procedura zabezpečení přijme a zpracuje strukturu MQCSP. Akce, jako je šifrování, jsou nevhodné pro jednu uživatelskou proceduru, protože neexistuje žádná uživatelská procedura pro provedení doplňkové akce.

Pokud nejsou nastavena pole SecurityParmsPtr a SecurityParmsOffset ve struktuře MQCNO a existuje uživatelská procedura zabezpečení na jednom nebo obou koncích kanálu, jsou volány uživatelské procedury nebo uživatelské procedury zabezpečení. Každá uživatelská procedura zabezpečení může vrátit svou vlastní strukturu MQCSP, která je adresována polem SecurityParmsPtr . Uživatelská procedura zabezpečení nebude znovu volána, dokud nebude ukončena (ExitReason z MQXR_TERM). Zapisovací program uživatelské procedury může uvolnit paměť používanou pro MQCSP v dané fázi.

Pokud instance kanálu připojení serveru sdílí více než jednu konverzaci, je vzor volání uživatelské procedury zabezpečení omezen na druhou a následující konverzaci.

Pro první konverzaci je vzor stejný, jako kdyby instance kanálu nesdílel konverzace. Pro druhou a následnou konverzaci není uživatelská procedura zabezpečení nikdy volána s MQXR_INIT, MQXR_INIT_SEC nebo MQXR_SEC_MSG. Volá se s MQXR_SEC_PARMS.

V instanci kanálu se sdílenými konverzacemi je MQXR_TERM volán pouze pro poslední spuštěnou konverzaci.

Každá konverzace má příležitost ve vyvolání MQXR_SEC_PARMS uživatelské procedury změnit MQCD; na konci připojení serveru kanálu může být tato funkce užitečná pro změnu například hodnot MCAUserIdentifier nebo LongMCAUserIdPtr před vytvořením připojení ke správci front.

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

Obrázek 4. Iniciovaná výměna připojení klienta se smlouvou pro připojení klienta pomocí parametrů zabezpečení

Poznámka: Aplikace uživatelské procedury zabezpečení vytvořené před vydáním produktu IBM WebSphere MQ 7.1 mohou vyžadovat aktualizaci. Další informace naleznete v tématu Programy uživatelských procedur pro zabezpečení zprávy kanálu.

ALW Identifikace volání API v programu uživatelské procedury pro odeslání nebo příjem

Používáte-li kanály MQI pro klienty, bajt 10 vyrovnávací paměti agenta identifikuje volání rozhraní API, které se používá při volání uživatelské procedury pro odeslání nebo příjem. To je užitečné pro identifikaci toho, které toky kanálů zahrnují uživatelská data a mohou vyžadovat zpracování, například šifrování nebo digitální podepisování.

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

Poznámka: Toto nejsou jediné hodnoty tohoto bajtu. Existují další **vyhrazené** hodnoty.

Tabulka 8. Identifikace volání rozhraní API		
Volání rozhraní API	**Hodnota bajtu 10 pro požadavek**	**Hodnota bajtu 10 pro odpověď**
MQCONN “1” na stránce 60, “2” na stránce 60	X'81 '	X' 91 '
MQDISC “1” na stránce 60	X'82 '	X' 92 '
MQOPEN “3” na stránce 60	X'83 '	X' 93 '
MQCLOSE	X'84 '	X' 94 '
MQGET “4” na stránce 60	X'85 '	X' 95 '
MQPUT “4” na stránce 60	X'86 '	X' 96 '
MQPUT1 “4” na stránce 60	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_prepare	X'A5'	X'B5'
Požadavek xa_commit	X'A6'	X'B6'
Požadavek xa_rollback	X'A7'	X'B7'
Požadavek xa_forget	X'A8'	X'B8'
Požadavek xa_recover	X'A9'	X'B9'
Požadavek xa_complete	X'AA'	X'BA '

Notes:

1. Připojení mezi klientem a serverem iniciuje klientská aplikace pomocí MQCONN. Proto, zejména pro tento příkaz, existuje několik dalších síťových toků. Totéž platí pro MQDISC, který ukončuje síťové připojení.
2. S MQCONNX se pro účely připojení klient-server zachází stejným způsobem jako s MQCONN.
3. Je-li otevřen rozsáhlý distribuční seznam, může pro každé volání MQOPEN existovat více než jeden tok sítě, aby bylo možné předat všechna požadovaná data do modulu MCA SVRCONN.
4. Velké zprávy mohou překročit velikost přenosového segmentu. Pokud k tomu dojde, může dojít k mnoha síťovým tokům, které jsou výsledkem jednoho volání rozhraní API.

z/OS Připojení klienta ke skupině sdílení front

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

Informace o této úloze

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

Klient vkládající do sdílené fronty se může připojit k libovolnému členovi skupiny sdílení front. Výhody připojení ke skupině sdílení front jsou možné zvýšení 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, že můžete vkládat zprávy do sdílené cílové fronty, což zvyšuje back-endovou dostupnost.

Připojení ke generickému rozhraní skupiny sdílení front otevře relaci s jedním ze správců front ve skupině. Tím se zvyšuje dostupnost front-endu, protože správce front klienta se může připojit k libovolným správcům front ve skupině. Ke skupině se připojujete pomocí generického rozhraní, pokud se nechcete připojit ke specifickému správci front v rámci skupiny sdílení front.

Generickým rozhraním může být adresa VIPA distributora prostředí sysplex nebo generický název prostředku VTAM nebo jiné společné rozhraní skupiny sdílení front. Další podrobnosti o nastavení generického rozhraní naleznete v tématu Nastavení komunikace pro IBM MQ for z/OS použití skupin sdílení front.

Postup

Chcete-li se připojit ke generickému rozhraní skupiny sdílení front, je třeba vytvořit definice kanálů, k nimž má přístup libovolný správce front ve skupině. Chcete-li to provést, musíte mít stejné definice pro každého správce front ve skupině.

1. Definujte kanál SVRCONN, jak ukazuje následující příklad:

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

   Definice kanálů na serveru jsou uloženy ve sdíleném úložišti Db2 . Každý správce front ve skupině sdílení front vytvoří lokální kopii definice a zajistí, že se při zadání volání MQCONN nebo MQCONNX budete vždy připojovat ke správnému kanálu připojení serveru.
2. Definujte kanál CLNTCONN, jak ukazuje následující příklad:

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

Výsledky

Vzhledem k tomu, že generické rozhraní skupiny sdílení front je uloženo v poli CONNAME v kanálu připojení klienta, můžete se nyní připojit k libovolnému správci front ve skupině a umístit jej do sdílených front vlastněných touto skupinou.

Použití proměnných prostředí IBM MQ

Pomocí příkazů můžete zobrazit aktuální nastavení nebo resetovat hodnoty proměnných prostředí IBM MQ .

Informace o této úloze

Proměnné prostředí můžete použít následujícími způsoby:

- Nastavení proměnných v profilu systému pro provedení trvalé změny
- Chcete-li zadat příkaz z příkazového řádku, chcete-li provést změnu pouze pro tuto relaci
- Chcete-li jedné nebo více proměnným přidělit konkrétní hodnotu závislou na spuštěné aplikaci, přidejte příkazy do skriptového souboru příkazů používaného aplikací.

Pro každou proměnnou prostředí můžete použít příkazy k zobrazení aktuálního nastavení nebo k resetování hodnoty proměnné prostředí. Tyto příkazy jsou k dispozici na všech podporovaných platformách, není-li uvedeno jinak. Formát příkazu závisí na vaší platformě. Příklad:

- Linux AIX V systému AIX and Linux:

```
export [environment variable]=value
```

- Windows V systému Windows:

```
Set [environment variable]=value
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(environment variable) VALUE(xx)
```

- MQ Appliance Informace o systému IBM MQ Appliancenaleznete v tématu Konfigurace proměnných prostředí v produktu IBM MQ Appliance v dokumentaci k produktu IBM MQ Appliance .

Kde je to možné, produkt IBM MQ použije výchozí hodnoty pro proměnné prostředí, které jste nenastavili.

Poznámka: z/OS Produkt IBM MQ for z/OS nepodporuje žádné proměnné prostředí IBM MQ . Používáte-li tuto platformu jako server, viz Tabulka definic kanálů klienta , kde naleznete informace o tom, jak je tabulka definic kanálů klienta generována v systému z/OS. Na platformě klienta můžete i nadále používat proměnné prostředí IBM MQ .

Procedura

- Windows
  V systému Windowspoužijte pro každou proměnnou prostředí následující příkazy k zobrazení aktuálního nastavení nebo k resetování hodnoty proměnné:
  - Chcete-li odebrat hodnotu proměnné prostředí, použijte následující příkaz:

    ```
    SET MQSERVER=
    ```

  - Chcete-li zobrazit aktuální nastavení proměnné prostředí, použijte následující příkaz:

    ```
    SET MQSERVER
    ```

  - Chcete-li zobrazit všechny proměnné prostředí pro relaci, použijte následující příkaz:

    ```
    set
    ```

- Linux AIX
  V systému AIX and Linuxpoužijte pro každou proměnnou prostředí následující příkazy k zobrazení aktuálního nastavení nebo k resetování hodnoty proměnné:
  - Chcete-li odebrat hodnotu proměnné prostředí, použijte následující příkaz:

    ```
    unset MQSERVER
    ```

  - Chcete-li zobrazit aktuální nastavení proměnné prostředí, použijte následující příkaz:

```
echo $MQSERVER
```

– Chcete-li zobrazit všechny proměnné prostředí pro relaci, použijte následující příkaz:

```
set
```

Související úlohy

Nastavení proměnných prostředí pro IBM MQ classes for JMS/Jakarta Messaging

Proměnné prostředí relevantní pro IBM MQ classes for Java

Definování dalších proměnných prostředí v souboru service.env

“Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83
Úpravou informací v konfiguračních souborech (`.ini`) můžete změnit chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovoval potřebám vaší instalace. Můžete také změnit volby konfigurace pro IBM MQ MQI clients.

Související odkazy

Použití proměnných prostředí ve vlastnostech MFT

Popisy proměnných prostředí

Popisy proměnných prostředí serveru a klienta, které jsou určeny pro použití zákazníkem.

Příklady použití

- Linux AIX V systémech AIX and Linux použijte tento formát: `export [environment variable]=value`.
- Windows V systémech Windows použijte tento formát: `Set [environment variable]=value`.
- IBM i V systémech IBM i použijte tento formát: `ADDENVVAR ENVVAR(environment variable) VALUE(xx)`.
- MQ Appliance Informace o systému IBM MQ Appliancenaleznete v tématu Konfigurace proměnných prostředí v produktu IBM MQ Appliance v dokumentaci k produktu IBM MQ Appliance .

AMQ_POVOLENÉ_ŠIFRY

Multi

V produktu IBM MQ 9.2.0můžete pomocí proměnné prostředí **AMQ_ALLOWED_CIPHERS** určit vlastní seznam specifikací CipherSpecs , které jsou povoleny pro použití s kanály IBM MQ na platformě Multiplatforms. Proměnná prostředí má stejné hodnoty jako atribut **AllowedCipherSpecs** sekce SSL souboru `.ini` :

- jeden název CipherSpec nebo
- Čárkami oddělený seznam názvů IBM MQ CipherSpec , které chcete znovu povolit, nebo
- Speciální hodnota `ALL`představující všechny CipherSpecs (nedoporučuje se).

Poznámka: Povolení volby **ALL** CipherSpecs se nedoporučuje, protože povolí protokoly SSL 3.0 a TLS 1.0 a velký počet slabých šifrovacích algoritmů.

Další informace naleznete v tématu Poskytnutí vlastního seznamu povolených CipherSpecs na platformě Multiplatforms v pořadí CipherSpec v rámci navázání komunikace TLS.

AMQ_BAD_COMMS_DATA_FDCS

Proměnná prostředí **AMQ_BAD_COMMS_DATA_FDCS** je platná, když je nastavena na libovolnou hodnotu.

Pokud jsou data, která produkt IBM MQ přijímá od hostitele přes protokol TCP/IP, v nesprávném formátu, například proto, že se síťový klient připojil k portu modulu listener produktu IBM MQ a pokusil se

komunikovat s nepodporovaným protokolem aplikace, zapíše správce front do protokolů chyb správce front chybovou zprávu AMQ9207E . Moduly listener produktu IBM MQ podporují připojení TCP/IP z agentů MCA (Message Channel Agent) správce front a z aplikací klienta MQI, JMS a XMS .

Poznámka: Moduly listener systému IBM MQ nepodporují aplikační protokol používaný klienty AMQP a MQTT. Tito klienti by se měli místo toho připojit k síťovým portům konfigurovaným v příslušném kanálu AMQP nebo službě telemetrie MQXR.

Může se také zapsat záznam zachycení dat selhání (FDC) obsahující neplatná data, která produkt IBM MQ přijal. Soubor FFST však není generován, pokud se jedná o začátek konverzace se vzdálenou stranou a formát je jednoduchý známý formát, jako např. požadavek GET z webového prohlížeče HTTP. Chcete-li toto potlačit, abyste způsobili zápis souborů FFST pro jakákoli chybná data včetně jednoduchých známých formátů, můžete nastavit proměnnou prostředí **AMQ_BAD_COMMS_DATA_FDCS** na libovolnou hodnotu (například TRUE) a restartovat správce front.

AMQ_CONVEBCDICNEWLINE

Pomocí proměnné prostředí **AMQ_CONVEBCDICNEWLINE** můžete určit, jak má IBM MQ převést znak NL EBCDIC na formát ASCII. Proměnná prostředí má stejné hodnoty jako atribut **ConvEBCDICNewline** souboru `mqs.ini`, tj. `NL_TO_LF`, `TABLE`nebo `ISO` (viz Všechny sekce správců front souboru mqs.ini). Můžete například použít proměnnou prostředí **AMQ_CONVEBCDICNEWLINE** namísto atributu stanza **ConvEBCDICNewline** , abyste poskytli funkčnost **ConvEBCDICNewline** na straně klienta v situacích, kdy nelze použít soubor `mqs.ini` . Pokud je nastaven atribut stanza i proměnná prostředí, má přednost atribut stanza.

Další informace viz Převod dat mezi kódovanými znakovými sadami .

AMQ_DIAGNOSTIC_MSG_SEVERITY

Je-li proměnná prostředí **AMQ_DIAGNOSTIC_MSG_SEVERITY** pro proces IBM MQ nastavena na hodnotu `1` , způsobí to, že se závažnost zprávy připojí k číslu zprávy jako jediný abecední znak velká písmena, když proces IBM MQ zapíše zprávu do protokolu chyb nebo do konzoly.

Chování, které produkt **AMQ_DIAGNOSTIC_MSG_SEVERITY** povoluje, je standardně nastaveno. Toto chování můžete vypnout nastavením proměnné prostředí na hodnotu `0`.

Další informace naleznete v tématu Použití protokolů chyb.

AMQ_DISABLE_CLIENT_AMS

Proměnnou prostředí **AMQ_DISABLE_CLIENT_AMS** můžete použít k zakázání funkce IBM MQ Advanced Message Security (AMS) na klientovi, pokud je při pokusu o připojení ke správci front z dřívější verze produktu nahlášena chyba `2085 (MQRC_UNKNOWN_OBJECT_NAME)` a používáte jednoho z následujících klientů:

- Java runtime environment (JRE) jiné než IBM Java runtime environment (JRE)
- Klient IBM MQ IBM MQ classes for JMS nebo IBM MQ classes for Java .

Poznámka: Pro klienty jazyka C nelze použít proměnnou prostředí **AMQ_DISABLE_CLIENT_AMS** . Místo toho musíte použít proměnnou prostředí **MQS_DISABLE_ALL_INTERCEPT** .

Další informace naleznete v tématu Zakázání rozšířeného zabezpečení zpráv v klientu.

AMQ_DMPMQCFG_QSGDISP_DEFAULT

Dotazy na dispozice správce front, které používá příkaz **dmpmqcfg** , standardně zjišťují pouze definice QSGDISP (QMGR). Další definice můžete zjistit pomocí proměnné prostředí **AMQ_DMPMQCFG_QSGDISP_DEFAULT** , kterou lze nastavit na jednu z následujících hodnot:

LIVE
Zahrnout pouze objekty definované s QSGDISP (QMGR) nebo QSGDISP (COPY).

ALL
Zahrnout objekty definované s QSGDISP (QMGR) a QSGDISP (COPY). Pokud je správce front členem skupiny sdílení front, jsou zahrnuty také QSGDISP (GROUP) a QSGDISP (SHARED).

COPY
Zahrnout pouze objekty definované pomocí QSGDISP (COPY)

SKUPINA
Zahrnout pouze objekty definované pomocí QSGDISP (GROUP); cílový správce front musí být členem skupiny sdílení front.

QMGR
Zahrnout pouze objekty definované s QSGDISP (QMGR). Toto je výchozí chování, pokud použijete tuto proměnnou prostředí tak, aby odpovídala existujícímu chování **dmpmqcfg**.

PRIVATE
Zahrnout pouze objekty definované s QSGDISP (QMGR) nebo QSGDISP (COPY).

SHARED
Zahrnout pouze objekty definované s QSGDISP (SHARED).

AMQ_IODELAY, AMQ_IODELAY_INMS a AMQ_IODELAY_FFST

Produkt IBM MQ zjistí, když operace čtení a zápisu do protokolu nebo vstupní a výstupní operace trvají déle, než se očekávalo. Může to být způsobeno problémy s operačním systémem nebo úložným systémem a může to mít vliv na výkon správce front. V produktu IBM MQ 9.3.4můžete použít proměnné prostředí **AMQ_IODELAY** k jemnému vyladění diagnostiky a časování, když je vstup a výstup pro protokol správce front a úložný systém souborů pomalý. Zobrazí-li se v protokolu chyb správce front zpráva AMQ6729W `Operace protokolu I/O překročila prahovou hodnotu` , zjistěte příčinu a proveďte příslušné úpravy. Použijte proměnné, jak je uvedeno v následujících příkladech:

AMQ_IODELAY
Prahová hodnota času v sekundách, předvolba je 1 sekunda. Pokud operace I/O trvá déle, než je tato prahová hodnota, je v souborech protokolu IBM MQ hlášena chybová zpráva `AMQ6729W` . Pokud prodlevy pokračují, varovná zpráva se opakuje nanejvýš každých 10 sekund. Tuto hodnotu můžete zvýšit, chcete-li potlačit chyby, nebo snížit, chcete-li vyšetřit specifické problémy s výkonem. Například:

```
export AMQ_IODELAY=200000
```

AMQ_IODELAY_INMS
Změňte časový ukazatel na mikrosekundy namísto sekund. Pomocí této volby můžete nastavit nižší prahovou hodnotu před získáním zprávy `AMQ6729` v protokolu správce front.

```
export AMQ_IODELAY_INMS=YES
```

AMQ_IODELAY_FFST
Kromě varovné zprávy v protokolu chyb je při každém překročení prahové hodnoty vygenerován soubor FFST obsahující diagnostické informace.

```
export AMQ_IODELAY_FFST=YES
```

Spuštění správce front jako v tomto příkladu způsobí zápis souboru FDC nebo FFST, pokud operace vstupu/výstupu trvá déle než 200000 mikrosekund (0.2s), což je stále poměrně velkorysá prahová hodnota.

Další informace naleznete v tématu Chování kontroly stavu správce front.

AMQ_LDAP_TRACE

Pokud je proměnná prostředí **AMQ_LDAP_TRACE** nastavena na nenulovou hodnotu, je možné zapnout a vypnout trasování klienta LDAP bez zastavení nebo spuštění správce front.

Další informace naleznete v tématu Povolení dynamického trasování kódu knihovny klienta LDAP.

METRIC_LICENCOVÁNÍ_AMQ_METRIKY

Multi

Nastavení proměnné prostředí **AMQ_LICENSING_METRIC=VPCMonthlyPeak** způsobí, že správce front odešle data související s měsíčními typy licencí VPC namísto výchozího chování při odesílání dat souvisejících s hodinovými licencemi založenými na kontejnerech.

Další informace o konfiguraci produktu IBM MQ pro použití se službou měření IBM Cloud Private naleznete v části IBM Cloud Private služba měření v dokumentaci k produktu IBM Cloud Private .

AMQ_MQS_INI_LOCATION

Linux AIX

Na systémech AIX and Linux můžete změnit umístění, které se používá pro soubor `mqs.ini` , nastavením umístění souboru `mqs.ini` v proměnné prostředí **AMQ_MQS_INI_LOCATION** . Tato proměnná prostředí musí být nastavena na úrovni systému.

Další informace o souboru `mqs.ini` , včetně umístění adresářů, naleznete v části IBM MQ configuration file, mqs.ini.

AMQ_NO_BAD_COMMS_DATA_FDCS

Proměnná prostředí **AMQ_NO_BAD_COMMS_DATA_FDCS** je platná, když je nastavena na libovolnou hodnotu.

Pokud produkt IBM MQ nerozpozná počáteční přenos dat při pokusu o připojení klienta jiného nežIBM MQ k modulu listener produktu IBM MQ TCP/IP, způsobí to, že správce front zapíše chybovou zprávu AMQ9207E do protokolů chyb správce front. Je také zapsán záznam zachycení dat selhání (FDC). Generování těchto diagnostických souborů můžete potlačit pomocí proměnné prostředí **AMQ_NO_BAD_COMMS_DATA_FDCS** . Je-li parametr **AMQ_NO_BAD_COMMS_DATA_FDCS** nastaven na libovolnou hodnotu (například TRUE), instruuje produkt IBM MQ , aby při vytváření sestav AMQ9207E chybových zpráv v počátečním toku komunikací negeneroval protokoly FFST. Aby byla proměnná prostředí efektivní, měla by být nastavena před spuštěním procesů správce front a modulu listener.

FDC je i nadále generováno v případě, že klient odesílá platné toky protokolu IBM MQ do správce front a poté odesílá neplatná data, protože to svědčí o problému klienta, který vyžaduje další zkoumání.

Poznámka: V systému IBM MQ 9.2.0je zachycení protokolů FFST při vytváření sestav AMQ9207E chybových zpráv v počátečních komunikačních tocích standardně potlačeno.

AMQ_NO_IPV6

Proměnná prostředí **AMQ_NO_IPV6** je platná, když je nastavena na libovolnou hodnotu. Je-li tato proměnná prostředí nastavena, zakáže použití parametru IPv6 při pokusu o připojení.

AMQ_REVERSE_COMMIT_ORDER

Proměnná prostředí **AMQ_REVERSE_COMMIT_ORDER** konfiguruje správce front tak, aby v transakci XA byla změna správce front IBM MQ potvrzena po dokončení příslušné aktualizace databáze. Aplikace, které čtou zprávy z front, zobrazí zprávu až po dokončení příslušné aktualizace databáze.

Poznámka: Nenastavujte parametr **AMQ_REVERSE_COMMIT_ORDER** , aniž byste přečetli a porozuměli scénáři, který je popsán v tématu Úroveň izolace.

AMQ_SSL_ALLOW_DEFAULT_CERT

Není-li proměnná prostředí **AMQ_SSL_ALLOW_DEFAULT_CERT** nastavena, může se aplikace připojit ke správci front s osobním certifikátem v úložišti klíčů klienta pouze v případě, že certifikát

obsahuje název popisku `ibmwebspheremq`*`userid`*. Když je nastavena proměnná prostředí **AMQ_SSL_ALLOW_DEFAULT_CERT** , certifikát nevyžaduje název popisku `ibmwebspheremq`*`userid`*. To znamená, že certifikát používaný pro připojení ke správci front může být výchozím certifikátem za předpokladu, že je v úložišti klíčů přítomen výchozí certifikát a úložiště klíčů neobsahuje osobní certifikát s předponou `ibmwebspheremq`*`userid`*.

Hodnota 1 povoluje použití výchozího certifikátu.

Namísto použití proměnné prostředí **AMQ_SSL_ALLOW_DEFAULT_CERT** může aplikace použít nastavení **CertificateLabel** sekce SSL v souboru `mqclient.ini` . Další informace viz Popisky digitálních certifikátů, základní informace o požadavcích a sekci SSL konfiguračního souboru klienta.

AMQ_SSL_LDAP_SERVER_VERSION

Proměnnou prostředí **AMQ_SSL_LDAP_SERVER_VERSION** lze použít k zajištění toho, aby server LDAP v2 nebo LDAP v3 používaly šifrovací komponenty IBM MQ v případech, kdy servery CRL vyžadují použití specifické verze protokolu LDAP.

Nastavte proměnnou prostředí na příslušnou hodnotu v prostředí, které se používá ke spuštění správce front nebo kanálu:

- Chcete-li požadovat, aby byl použit protokol LDAP v2 , nastavte `AMQ_SSL_LDAP_SERVER_VERSION=2`.
- Chcete-li požadovat, aby byl použit protokol LDAP v3 , nastavte `AMQ_SSL_LDAP_SERVER_VERSION=3`.

Tato proměnná prostředí nemá vliv na připojení LDAP zavedená správcem front IBM MQ pro ověřování uživatelů nebo autorizaci uživatelů.

AMQ_USE_ZLIBNX

AIX V 9.3.0

V systému AIXlze proměnnou prostředí **AMQ_USE_ZLIBNX** použít k povolení agentů MCA (message channel agents) používat knihovnu zlibNX s hardwarovou akcelerací pro kompresi a dekompresi dat zpráv při použití technik ZLIBFAST nebo ZLIBHIGH.

Tip: Vysoce komprimovatelné zprávy, jejichž velikost přesahuje 2 kB, mohou s největší pravděpodobností těžit z použití knihovny zlibNX snížením využití procesoru.

Knihovna zlibNX je k dispozici v produktu IBM AIX 7.2 s balíkem Technology Level 4 Expansion Pack a novějším. Pokud je nastavena proměnná prostředí a knihovna zlibNX (`/usr/opt/zlibNX/lib/libz.a`) není nainstalována, agenti kanálu zpráv budou používat standardní knihovnu zlib poskytnutou v instalaci produktu IBM MQ for AIX .

HOME

Linux IBM i AIX

V systémech AIX, Linux a IBM iproměnná prostředí **HOME** uvádí název adresáře, který se hledá pro soubor `mqclient.ini` . Tento soubor obsahuje informace o konfiguraci používané produktem IBM MQ MQI clients.

Další informace viz IBM MQ Konfigurační soubor klienta MQI, mqclient.ini a Umístění konfiguračního souboru klienta.

HOMEDRIVE a HOMEPATH

Windows

Chcete-li je použít, musí být nastaveny proměnné prostředí **HOMEDRIVE** i **HOMEPATH** . Používají se na systémech Windows k uvedení názvu adresáře, který se prohledává pro soubor `mqclient.ini` . Tento soubor obsahuje informace o konfiguraci používané produktem IBM MQ MQI clients.

Další informace viz IBM MQ Konfigurační soubor klienta MQI, mqclient.ini a Umístění konfiguračního souboru klienta.

LDAP_BASEDN

LDAP_BASEDN je požadovaná proměnná prostředí pro spuštění ukázkového programu LDAP. Určuje základní rozlišující název pro hledání v adresáři.

LDAP_HOST

LDAP_HOST je volitelná proměnná prostředí pro spuštění ukázkového programu LDAP. Určuje název hostitele, na kterém je spuštěn server LDAP; není-li uveden, použije se jako výchozí lokální hostitel.

LDAP_VERSION

LDAP_VERSION je volitelná proměnná prostředí pro spuštění ukázkového programu LDAP. Uvádí verzi protokolu LDAP, která se má použít, a může být buď 2, nebo 3. Většina serverů LDAP nyní podporuje verzi 3 protokolu; všechny podporují starší verzi 2. Tato ukázka funguje stejně dobře s libovolnou verzí protokolu, a pokud není určena, standardně se použije verze 2.

MQ_CHANNEL_SUPPRESS_INTERVAL

Proměnná prostředí **MQ_CHANNEL_SUPPRESS_INTERVAL** určuje časový interval v sekundách, během kterého mají být zprávy definované pomocí produktu **MQ_CHANNEL_SUPPRESS_MSGS** potlačeny z zápisu do protokolu chyb, spolu s počtem případů, kdy bude povoleno, aby se zpráva vyskytla během uvedeného časového intervalu, než bude potlačena. Výchozí hodnota je 60,5, což znamená, že všechny další výskyty dané zprávy jsou potlačeny po prvních pěti výskytech této zprávy v 60sekundovém intervalu. Další informace naleznete v tématu Potlačení chybových zpráv kanálu z protokolů chyb na platformě Multiplatforms.

Proměnná prostředí **MQ_CHANNEL_SUPPRESS_INTERVAL** je srovnatelná s proměnnou prostředí SuppressInterval v souboru `qm.ini` .

MQ_CHANNEL_SUPPRESS_MSGS

Proměnná prostředí **MQ_CHANNEL_SUPPRESS_MSGS** potlačuje chybové zprávy kanálu v protokolu chyb. Můžete určit seznam zpráv, které jsou potlačeny. Parametr **MQ_CHANNEL_SUPPRESS_MSGS** se používá ve spojení s parametrem **MQ_CHANNEL_SUPPRESS_INTERVAL**, který určuje, kolikrát se každá zpráva objeví před potlačením, a dobu, po kterou jsou zprávy potlačeny. Další informace naleznete v tématu Potlačení chybových zpráv kanálu z protokolů chyb na platformě Multiplatforms.

Proměnná prostředí **MQ_CHANNEL_SUPPRESS_MSGS** je srovnatelná s proměnnou prostředí SuppressMessage v souboru `qm.ini` s tou výjimkou, že můžete potlačit libovolnou zprávu kanálu pomocí proměnné prostředí, zatímco pro metodu `qm.ini` existuje omezující seznam.

MQ_CONNECT_TYPE

Multi

Na platformě Multiplatforms můžete použít proměnnou prostředí **MQ_CONNECT_TYPE** v kombinaci s typem vazby určeným v poli Volby ve struktuře MQCNO, která se používá ve volání MQCONNX. Parametr **MQ_CONNECT_TYPE** má vliv pouze na vazby typu STANDARD. Pro ostatní vazby je parametr **MQ_CONNECT_TYPE** ignorován.

Další informace naleznete v tématu Použití voleb volání MQCONNX s parametrem MQ_CONNECT_TYPE.

MQ_CROSS_QUEUE_ORDER_ALL

Nastavíte-li proměnnou prostředí **MQ_CROSS_QUEUE_ORDER_ALL** na nenulovou hodnotu, bude pořadí vložení zprávy udržováno v pracovní jednotce. To znamená, že pokud jsou zprávy v jednotce práce (UoW) vloženy do více front (například Q1, pak Q2), když je vydán MQCMIT, jsou zprávy doručeny a zpřístupněny ve stejném pořadí fronty, ve kterém byly PUT.

V prostředí s více správci front musí produkt **MQ_CROSS_QUEUE_ORDER_ALL** před spuštěním každého správce front existovat a mít neprázdnou hodnotu na straně odesílání i příjmu.

MQ_EPHEMERAL_PREFIX

Proměnná prostředí **MQ_EPHEMERAL_PREFIX** určuje cestu k dočasnému adresáři správce front, v němž jsou uchovávána data správce front, zatímco je správce front spuštěn.

Jako alternativu ke změně dočasné předpony změnou atributu **EphemeralPrefix** v atributu **DefaultEphemeralPrefix** sekce AllQueueManagers souboru `mqs.ini` můžete použít proměnnou prostředí **MQ_EPHEMERAL_PREFIX** k přepsání atributu **EphemeralPrefix** pro příkaz **crtmqm** . Další informace viz Konfigurovatelný dočasný adresář.

MQ_FILE_PATH

Windows

Proměnná prostředí **MQ_FILE_PATH** je konfigurována během instalace běhového balíku na platformě Windows . Tato proměnná prostředí obsahuje stejná data jako následující klíč v registru Windows :

```
HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere MQ\Installation\InstallationName\FilePath
```

Další informace viz setmqenv (nastavit prostředí IBM MQ) a crtmqenv (vytvořit prostředí IBM MQ).

MQ_JAVA_DATA_PATH

Proměnná prostředí **MQ_JAVA_DATA_PATH** uvádí adresář pro výstup protokolu a trasování pro IBM MQ classes for JMS a IBM MQ classes for Jakarta Messaging a IBM MQ classes for Java. Používají jej skripty dodávané s produktem IBM MQ classes for JMS a IBM MQ classes for Jakarta Messaging a IBM MQ classes for Java.

Další informace naleznete v tématu Nastavení proměnných prostředí pro třídy IBM MQ pro systém zpráv JMS/Jakarta a Proměnné prostředí relevantní pro třídy IBM MQ pro jazyk Java.

MQ_JAVA_INSTALL_PATH

Proměnná prostředí **MQ_JAVA_INSTALL_PATH** určuje adresář, ve kterém jsou nainstalovány produkty IBM MQ classes for JMS a IBM MQ classes for Jakarta Messaging , jak je uvedeno v části Co je instalováno pro třídy IBM MQ pro platformu JMS, a adresář IBM MQ classes for Java , jak je uvedeno v části IBM MQ classes for Java instalační adresáře .

Další informace naleznete v tématu Nastavení proměnných prostředí pro třídy IBM MQ pro systém zpráv JMS/Jakarta a Proměnné prostředí relevantní pro třídy IBM MQ pro jazyk Java.

MQ_JAVA_LIB_PATH

Proměnná prostředí **MQ_JAVA_LIB_PATH** uvádí adresář, kde jsou uloženy knihovny IBM MQ classes for JMS a IBM MQ classes for Jakarta Messaginga knihovny IBM MQ classes for Java . Některé skripty, například `IVTRun`, které jsou dodávány s IBM MQ classes for JMS a IBM MQ classes for Jakarta Messaging nebo proměnnou prostředí IBM MQ classes for Java , používají tuto proměnnou prostředí.

Další informace naleznete v tématu Nastavení proměnných prostředí pro třídy IBM MQ pro systém zpráv JMS/Jakarta a Proměnné prostředí relevantní pro třídy IBM MQ pro jazyk Java.

MQ_OVERRIDE_DATA_PATH

Pomocí proměnné prostředí **MQ_OVERRIDE_DATA_PATH** můžete změnit výchozí adresář cesty k datům IBM MQ .

MQ_SET_NODELAYACK

AIX

Proměnná prostředí **MQ_SET_NODELAYACK** vypne zpožděné potvrzení TCP na systému AIX.

Nastavíte-li tuto proměnnou prostředí, nastavení vypne zpožděné potvrzení TCP voláním volání setsockopt operačního systému s volbou TCP_NODELAYACK . Tuto funkci podporuje pouze produkt AIX , takže proměnná prostředí **MQ_SET_NODELAYACK** má vliv pouze na AIX.

MQ_USER_NAME

Linux

Pomocí proměnné prostředí **MQ_USER_NAME** můžete povolit odregistrovanou instalaci v systému Linux a zvolit jméno nepojmenovaného uživatele. To je třeba například pro použití hierarchií publikování/odběru v produktu OpenShift.

Hodnota **MQ_USER_NAME** se nesmí shodovat s již existujícím uživatelem v systému a musí být menší nebo rovna 12 bajtům.

MQAPI_TRACE_LOGFILE

Ukázkový uživatelský program rozhraní API generuje trasování MQI do souboru určeného uživatelem s předponou, která je definována v proměnné prostředí **MQAPI_TRACE_LOGFILE** .

Další informace viz Ukázkový program uživatelské procedury rozhraní API.

MQAPPLNAME

ALW

Pokud dosud nebyl vybrán název aplikace, můžete jako název, který má být použit k identifikaci připojení ke správci front, použít proměnnou prostředí **MQAPPLNAME** . Použije se pouze prvních 28 znaků a nesmí to být všechny mezery nebo hodnoty null.

Další informace naleznete v tématu Použití názvu aplikace v podporovaných programovacích jazycích.

MQCCSID

Proměnná prostředí **MQCCSID** uvádí číslo kódované znakové sady, které se má použít, a přepisuje hodnotu CCSID, se kterou byl server nakonfigurován. **MQCCSID** lze použít k přepsání nativního CCSID aplikace a uvést číslo kódované znakové sady, které se má použít, například pokud je nativní CCSID nepodporovaný CCSID nebo není požadovaný CCSID.

Chcete-li nastavit **MQCCSID**, použijte jeden z následujících příkazů:

- Linux AIX V systému AIX and Linux:

```
export MQCCSID=number
```

- Windows V systému Windows:

```
SET MQCCSID=number
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQCCSID) VALUE(number)
```

Další informace viz Výběr CCSID klienta nebo serveru.

MQCCDTURL

Proměnná prostředí **MQCCDTURL** poskytuje ekvivalentní schopnost nastavení kombinace proměnných prostředí **MQCHLLIB** a **MQCHLTAB** . Umožňuje vám poskytnout soubor, ftp nebo http adresu URL jako jedinou hodnotu, ze které lze získat tabulku definic kanálů klienta pro nativní programy, které se připojují jako klienti, tj. aplikace C, COBOL nebo C + +.

Poznámka: Použití proměnných prostředí k poskytnutí adresy URL nemá žádný vliv na aplikace Java, JMS nebo spravované .NET .

Produkt IBM MQ podporuje načítání tabulky CCDT ze souboru, adresy URL protokolu FTP nebo http. Produkt **MQCCDTURL** však přijímá pouze hodnotu adresy URL. Nepřijímá existující formát adresáře lokálního systému souborů.

Chcete-li použít **MQCCDTURL** místo **MQCHLLIB** a **MQCHLTAB** s lokálním souborem, můžete použít protokol `'file://'` . Proto, jak je uvedeno v tomto příkladu pro AIX a Linux:

```
export MQCCDTURL=file:///var/mqm/qmgrs/QMGR/@ipcc/MYCHL.TAB
```

je ekvivalentní:

```
export MQCHLLIB=/var/mqm/qmgrs/QMGR/@ipcc
export MQCHLTAB=MYCHL.TAB
```

Můžete také uvést soubor JSON, jak je zobrazeno v tomto příkladu pro Windows:

```
set MQCCDTURL=file:/c:/mq-channels/CCDT-QMGR1.json
```

je ekvivalentní:

```
set MQCHLLIB=C:\mq-channels
set MQCHLTAB=CCDT-QMGR1.json
```

Další informace viz Přístup URL k tabulce CCDT.

MQCERTLABL

Proměnná prostředí **MQCERTLABL** definuje popisek certifikátu definice kanálu pro produkt IBM MQ , který se má použít k vyhledání osobního certifikátu odeslaného během navázání komunikace TLS.

Další informace naleznete v tématu Popisky digitálních certifikátů, základní informace o požadavcích.

MQCERTVPOL

Proměnná prostředí **MQCERTVPOL** uvádí typ zásady ověření platnosti certifikátu, která se má použít. Tato proměnná prostředí přepíše atribut **CertificateValPolicy** v sekci SSL konfiguračního souboru klienta.

MQCERTVPOL lze nastavit na jednu ze dvou hodnot:

ANY
Použijte libovolnou zásadu ověření certifikátu, která je podporována základní knihovnou zabezpečených soketů. Toto nastavení je výchozí.

RFC5280
Použijte pouze ověření certifikátu, které vyhovuje standardu RFC 5280.

Chcete-li nastavit **MQCERTVPOL**, použijte jeden z těchto příkazů:

- Linux AIX Pro systémy AIX and Linux :

  ```
  export MQCERTVPOL= value
  ```

- Windows Pro systémy Windows :

```
SET MQCERTVPOL= value
```

- IBM i Pro systémy IBM i :

```
ADDENVVAR ENVVAR(MQCERTVPOL) VALUE(value)
```

Další informace naleznete v tématu Zásady ověřování certifikátů v produktu IBM MQ a Konfigurace zásad ověřování certifikátů v produktu IBM MQ.

MQCHLLIB

Proměnná prostředí **MQCHLLIB** určuje cestu k adresáři souboru, který obsahuje tabulku CCDT (Client Channel Definition Table). Soubor je vytvořen na serveru, ale lze jej zkopírovat na pracovní stanici IBM MQ MQI client .

Chcete-li nastavit **MQCHLLIB**, použijte jeden z těchto příkazů:

- Windows V systému Windows:

```
SET MQCHLLIB=pathname
```

  Příklad:

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

- Linux AIX Pro systémy AIX and Linux :

```
export MQCHLLIB=pathname
```

- IBM i Pro IBM i:

```
ADDENVVAR ENVVAR(MQCHLLIB) VALUE(pathname)
```

Není-li parametr **MQCHLLIB** nastaven, výchozí cesta pro klienta je:

- Linux AIX V systému AIX and Linux: `/var/mqm/`
- Windows V systému Windows: *MQ_INSTALLATION_PATH*
- IBM i V systému IBM i: `/QIBM/UserData/mqm/`

Pro příkazy **crtmqm** a **strmqm** je cesta standardně nastavena na jednu ze dvou sad cest. Je-li nastavena hodnota *datapath* , výchozí hodnota cesty je jedna z prvních sad. Není-li parametr *datapath* nastaven, výchozí hodnota cesty je jedna z druhé sady.

- Linux AIX V systému AIX and Linux: *datapath*`/@ipcc`
- Windows V systému Windows: *datapath*`\@ipcc`
- IBM i V systému IBM i: *datapath*`/&ipcc`

Nebo:

- Linux AIX V systému AIX and Linux: `/prefix/qmgrs/`*qmgrname*`/@ipcc`

- Windows V systému Windows: *MQ_INSTALLATION_PATH*\data\qmgrs*qmgrname*\@ipcc
- IBM i V systému IBM i: /*prefix*/qmgrs/*qmgrname*/&ipcc

kde:

- *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .
- Pokud je přítomen, *datapath* je hodnota DataPath definovaná v sekci správce front.
- *prefix* je hodnota předpony definovaná v sekci správce front. Předpona je obvykle jedna z následujících hodnot:
  - Linux AIX /var/mqm na systémech AIX and Linux .
  - IBM i /QIBM/UserData/mqm/ zapnuto IBM i.
- *qmgrname* je hodnota atributu Directory definovaná v sekci správce front. Hodnota se může lišit od skutečného názvu správce front. Hodnota mohla být pozměněna, aby nahradila speciální znaky.
- Kde je definována sekce správce front, závisí na platformě:
  - Linux IBM i AIX V souboru mqs.ini na adrese IBM i, AIX and Linux.
  - Windows V registru na systému Windows.

Notes:

1. z/OS Používáte-li jako server IBM MQ for z/OS , musí být soubor uchováván na pracovní stanici klienta IBM MQ .
2. Je-li nastaveno, MQCHLLIB přepíše cestu použitou k vyhledání tabulky CCDT.
3. MQCHLLIB může obsahovat adresu URL, která pracuje v kombinaci s proměnnou prostředí MQCHLTAB (viz “Přístup URL k tabulce CCDT” na stránce 52).
4. Proměnné prostředí, jako např. **MQCHLLIB**, mohou být vymezeny pro proces, úlohu nebo pro celý systém způsobem specifickým pro platformu.
5. Pokud na serveru nastavíte celý systém **MQCHLLIB** , nastaví stejnou cestu k souboru CCDT pro všechny správce front na serveru. Pokud nenastavíte proměnnou prostředí **MQCHLLIB** , bude cesta pro každého správce front odlišná. Správci front načtou hodnotu **MQCHLLIB**, je-li nastavena, v příkazu **crtmqm** nebo **strmqm** .
6. Pokud na jednom serveru vytvoříte více správců front, je toto rozlišení důležité z následujícího důvodu. Pokud nastavíte volbu **MQCHLLIB** pro celý systém, každý správce front aktualizuje stejný soubor CCDT. Soubor obsahuje definice připojení klienta ze všech správců front na serveru. Pokud stejná definice existuje ve více správcích front, například SYSTEM.DEF.CLNTCONN , soubor obsahuje nejnovější definici. Je-li při vytváření správce front nastaven parametr **MQCHLLIB** , bude v tabulce CCDT aktualizován soubor SYSTEM.DEF.CLNTCONN . Aktualizace přepíše soubor SYSTEM.DEF.CLNTCONN vytvořený jiným správcem front. Pokud jste upravili předchozí definici, vaše úpravy budou ztraceny. Z tohoto důvodu musíte zvážit nalezení alternativ k nastavení **MQCHLLIB** jako proměnné prostředí pro celý systém na serveru.
7. Volba MQSC a PCF NOREPLACE v definici připojení klienta nekontroluje obsah souboru CCDT. Bez ohledu na volbu NOREPLACE bude nahrazena definice kanálu připojení klienta se stejným názvem, který byl vytvořen dříve, ale nikoli tímto správcem front. Pokud byla definice dříve vytvořena stejným správcem front, definice nebude nahrazena.
8. Příkaz **rcrmqobj** -t clchltab odstraní a znovu vytvoří soubor CCDT. Soubor je znovu vytvořen pouze s definicemi připojení klienta vytvořenými ve správci front, pro kterého je příkaz spuštěn.
9. Další příkazy, které aktualizují tabulky CCDT, upravují pouze kanály připojení klienta, které mají stejný název kanálu. Ostatní kanály připojení klienta v souboru nejsou změněny.
10. Cesta pro **MQCHLLIB** nepotřebuje uvozovky.

Další informace naleznete v tématu Umístění tabulky CCDT, Přístup k adrese URL tabulky CCDTa Připojení klientských aplikací ke správcům front pomocí proměnných prostředí.

MQCHLTAB

Proměnná prostředí **MQCHLTAB** určuje název souboru, který obsahuje tabulku CCDT (Client Channel Definition Table). Výchozí název souboru je AMQCLCHL.TAB.

Chcete-li nastavit **MQCHLTAB**, použijte jeden z těchto příkazů:

- Linux AIX V systému AIX and Linux:

```
export MQCHLTAB=filename
```

- Windows V systému Windows:

```
SET MQCHLTAB=filename
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQCHLTAB) VALUE(filename)
```

Příklad:

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

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

Další informace naleznete v tématu Umístění tabulky CCDT, Přístup k adrese URL tabulky CCDTa Připojení klientských aplikací ke správcům front pomocí proměnných prostředí.

MQCLNTCF

Proměnná prostředí **MQCLNTCF** určuje umístění konfiguračního souboru IBM MQ MQI client . Tento soubor obsahuje informace o konfiguraci používané produktem IBM MQ MQI clients.

Pomocí proměnné prostředí **MQCLNTCF** můžete upravit cestu k souboru `mqclient.ini` .

Formát této proměnné prostředí je úplná adresa URL. To znamená, že název souboru nemusí být nutně `mqclient.ini`, což usnadňuje umístění souboru do systému souborů připojeného k síti. Další informace viz IBM MQ Konfigurační soubor klienta MQI, mqclient.ini a Umístění konfiguračního souboru klienta.

MQDOTNET_TRACE_ON

Proměnná prostředí **MQDOTNET_TRACE_ON** se používá k povolení trasování pro redistribuovatelné klienty produktu IBM MQ .NET . Hodnoty menší než 0 nepovolují trasování, 1 povolují výchozí trasování a hodnoty větší než 1 povolují podrobné trasování.

Další informace viz Trasování IBM MQ .NET aplikace a Trasování IBM MQ .NET aplikace používající proměnné prostředí.

MQIPADDRV

Proměnná prostředí **MQIPADDRV** určuje, který protokol IP se má použít pro připojení kanálu. Má možné řetězcové hodnoty `"MQIPADDR_IPV4"` nebo `"MQIPADDR_IPV6"`. Tyto hodnoty mají stejný význam jako IPv4 a IPv6 v **ALTER QMGR IPADDRV** a atribut **IPAddressVersion** sekce TCP konfiguračního souboru klienta. Není-li proměnná prostředí nastavena, předpokládá se `"MQIPADDR_IPV4"` .

Chcete-li nastavit **MQIPADDRV**, použijte jeden z těchto příkazů:

- Linux AIX V systému AIX and Linux:

```
export MQIPADDRV=MQIPADDR_IPV4|MQIPADDR_IPV6"/>
```

- Windows V systému Windows:

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

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQIPADDRV) VALUE(MQIPADDR_IPV4|MQIPADDR_IPV6)
```

MQKEYRPWD

V 9.3.0 V 9.3.0

Když nastavíte proměnnou prostředí *MQKEYRPWD* , uvádí heslo pro úložiště klíčů, které obsahuje digitální certifikát patřící uživateli. Pokud použijete volbu *MQKEYRPWD* , musíte před nastavením hodnoty proměnné prostředí zašifrovat heslo.

Chcete-li nastavit *MQKEYRPWD*, použijte jeden z těchto příkazů:

- Linux AIX Na systémech AIX and Linux:

```
export MQKEYRPWD=passphrase
```

- Windows Na systémech Windows:

```
SET MQKEYRPWD=passphrase
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQKEYRPWD) VALUE(passphrase)
```

Pro tuto proměnnou prostředí neexistuje žádná výchozí hodnota.

V 9.3.0 V 9.3.0 Další informace naleznete zde:

- ALW Dodání hesla úložiště klíčů pro IBM MQ MQI client on AIX, Linux, and Windows a Šifrování hesla úložiště klíčů
- IBM i Zadejte heslo úložiště klíčů pro IBM MQ MQI client on IBM i a Šifrování hesla úložiště klíčů.

MQLICENSE

Linux

Na systémech Linux můžete použít proměnnou prostředí **MQLICENSE** k přijetí nebo zobrazení licence na produkt IBM MQ po instalaci produktu.

Další informace o tom, proč to chcete nebo potřebujete udělat, naleznete v tématu Přijetí licence na webu IBM MQ pro Linux .

Proměnnou prostředí **MQLICENSE** lze nastavit na jednu ze dvou hodnot:

Přijmout
Přijměte licenci po instalaci.

zobrazit
Zobrazit licenci, pokud byla licence přijata.

Chcete-li přijmout licenci po instalaci, použijte tento příkaz:

```
export MQLICENSE=accept
```

Chcete-li zobrazit licenci, použijte tento příkaz:

```
export MQLICENSE=view
```

Poznámka: K přijetí a zobrazení licence můžete také použít následující příkazy:

- mqlicense (přijměte licenci po instalaci)
- dspmqlic (zobrazit IBM MQ licenci)

MQMAXERRORLOGSIZE

Proměnná prostředí **MQMAXERRORLOGSIZE** určuje velikost protokolu chyb správce front, který je zkopírován do zálohy.

Další informace naleznete v tématu Použití protokolů chyb.

MQNAME

Proměnná prostředí **MQNAME** uvádí lokální název systému NetBIOS , který mohou používat procesy IBM MQ . Připojení NetBIOS se vztahuje pouze na klienta a server, na kterém běží produkt Windows.

Chcete-li nastavit **MQNAME**, použijte tento příkaz:

```
SET MQNAME=Your_env_Name
```

Příklad:

```
SET MQNAME=CLIENT1
```

Některé implementace systému NetBIOS vyžadují jedinečný název nastavený pomocí **MQNAME**pro každou aplikaci, pokud spouštíte více aplikací IBM MQ současně na serveru IBM MQ MQI client.

Další informace viz Definování názvu IBM MQ lokálního NetBIOS.

MQNOREMPOOL

Když nastavíte proměnnou prostředí **MQNOREMPOOL** , vypne sdružování kanálů a způsobí, že kanály budou spuštěny jako podprocesy modulu listener.

Další informace viz MCATYPE (Typ agenta kanálu zpráv).

MQPSE_TRACE_LOGFILE

Proměnnou prostředí **MQPSE_TRACE_LOGFILE** použijete při spuštění ukázkového programu uživatelské procedury publikování AMQSPSE0, což je ukázkový program jazyka C uživatelské procedury, který zachycuje publikování před jeho doručením odběrateli. V procesu aplikace, který má být trasován, tato proměnná prostředí popisuje, kam musí být zapisovány trasovací soubory.

Další informace viz Ukázkový program uživatelské procedury publikování.

MQS_AMSCRED_KEYFILE

Pomocí proměnné prostředí **MQS_AMSCRED_KEYFILE** můžete přepsat nebo poskytnout počáteční soubor s klíči, který se má použít za běhu aplikací IBM MQ Advanced Message Security (AMS), nebo když chráníte konfigurační soubor úložiště klíčů pomocí příkazu **runamscred** .

Další informace naleznete v tématu Použití úložišť klíčů a certifikátů s produktem AMS a Ochrana hesel v IBM MQ konfiguračních souborech komponenty.

MQS_DISABLE_ALL_INTERCEPT

Proměnnou prostředí **MQS_DISABLE_ALL_INTERCEPT** můžete použít k zakázání IBM MQ Advanced Message Security (AMS), pokud je při pokusu o připojení ke správci front z dřívější verze produktu nahlášena chyba 2085 (MQRC_UNKNOWN_OBJECT_NAME) a používáte produkt IBM MQ s nativními klienty C.

Poznámka: Proměnnou prostředí **MQS_DISABLE_ALL_INTERCEPT** můžete použít pouze pro klienty jazyka C. U klientů systému Java musíte místo toho použít proměnnou prostředí **AMQ_DISABLE_CLIENT_AMS** .

Další informace naleznete v tématu Zakázání rozšířeného zabezpečení zpráv v klientu.

MQS_IPC_HOST

Vzhledem k tomu, že objekty systému souborů IPC musí být rozlišeny systémem, je do cesty k adresáři přidán podadresář pro každý systém, na kterém je spuštěn správce front. Pokud vygenerovaná hodnota názvu hostitele vytvoří problém, můžete název hostitele nastavit pomocí proměnné prostředí **MQS_IPC_HOST** .

Další informace naleznete v tématu Sdílení souborů IBM MQ na platformě Multiplatforms.

MQS_KEYSTORE_CONF

Proměnná prostředí **MQS_KEYSTORE_CONF** určuje umístění konfiguračního souboru úložiště klíčů pro IBM MQ Advanced Message Security (AMS), pokud soubor není ve výchozím umístění *home_directory*/.mqs/keystore.conf.

Další informace naleznete v tématu Použití úložišť klíčů a certifikátů s produktem AMS.

Máte-li problémy se systémem Managed File Transfer, prohlédněte si téma Odstraňování problémů, když MFT nečte vlastnosti úložiště klíčů pro AMS.

MQS_MQI_KEYFILE

V 9.3.0 V 9.3.0

Když nastavíte proměnnou prostředí **MQS_MQI_KEYFILE** , uvádí umístění počátečního souboru s klíči, který obsahuje počáteční klíč, který se má použít pro operace ochrany heslem. Není-li uveden počáteční soubor s klíči, systém ochrany heslem IBM MQ použije výchozí počáteční klíč.

Chcete-li nastavit **MQS_MQI_KEYFILE**, použijte jeden z těchto příkazů:

- Linux AIX Na systémech AIX and Linux:

```
export MQS_MQI_KEYFILE=key file location
```

- Windows Na systémech Windows:

```
SET MQS_MQI_KEYFILE=key file location
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQS_MQI_KEYFILE) VALUE(key file location)
```

V 9.3.0 V 9.3.0 Další informace naleznete v tématu Poskytnutí počátečního klíče pro IBM MQ MQI client on AIX, Linux, and Windows a Poskytnutí počátečního klíče pro IBM MQ MQI client on IBM i.

MQS_SSLCRYP_KEYFILE

V 9.3.0

Proměnná prostředí **MQS_SSLCRYP_KEYFILE** je alternativní způsob, jak zadat úplnou cestu a název souboru obsahujícího počáteční klíč použitý k zašifrování hesla v řetězci konfigurace šifrovacího hardwaru PKCS #11 , místo toho, abyste jej uvedli s atributem **SSLCryptoHardwareKeyFile** v sekci SSL `qm.ini`. Produkt **MQS_SSLCRYP_KEYFILE** má vyšší prioritu než soubor `qm.ini` , takže jeho hodnota má přednost před jakoukoli jinou hodnotou. Další informace viz IBM MQ klienti používající kryptografický hardware.

MQS_TRACE_OPTIONS

AIX

Pro výběrové trasování komponent v systému AIXpoužijte proměnnou prostředí **MQS_TRACE_OPTIONS** , abyste jednotlivě aktivovali funkce trasování s vysokými podrobnostmi a parametry.

Poznámka: Nastavte proměnnou prostředí **MQS_TRACE_OPTIONS** pouze v případě, že jste byli instruováni podporou IBM .

Další informace naleznete v tématu Trasování na serveru AIX and Linux.

MQSERVER

Proměnná prostředí **MQSERVER** se používá k definování minimálního kanálu. **MQSERVER** uvádí umístění serveru IBM MQ a komunikační metodu, která se má použít.

Poznámka: Produkt **MQSERVER** nelze použít k definování kanálu TLS nebo kanálu s ukončením kanálu. Další informace o definování kanálu TLS naleznete v tématu Ochrana kanálů pomocí protokolu TLS.

Následující příklady ukazují, jak nastavit **MQSERVER**:

- Linux AIX V systému AIX and Linux:

```
export  MQSERVER='SYSTEM.DEF.SVRCONN/TCP/AMACHINE.ACOMPANY.COM(1414)'
```

- Windows V systému Windows:

```
SET  MQSERVER=SYSTEM.DEF.SVRCONN/TCP/AMACHINE.ACOMPANY.COM(1414)
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQSERVER) VALUE('SYSTEM.DEF.SVRCONN/TCP/AMACHINE.ACOMPANY.COM(1414)')
```

Poznámka:

- Název kanálu nemůže obsahovat dopředné lomítko (/), protože tento znak slouží k oddělení názvu kanálu, typu transportu a názvu připojení. Když se proměnná prostředí **MQSERVER** používá k definování kanálu klienta, použije se maximální délka zprávy (MAXMSGL) 100 MB. Proto je maximální velikost zprávy platná pro kanál hodnotou určenou v kanálu SVRCONN na serveru.
- Typ přenosu může být `LU62` , `TCP` , NETBIOS, SPX, v závislosti na platformě klienta IBM MQ .
- Název připojení musí být úplný název sítě. například `AMACHINE.ACOMPANY.COM(1414)`.

- Název připojení může být seznam názvů připojení oddělených čárkami. Názvy připojení v seznamu se používají podobným způsobem jako více připojení v tabulce připojení klienta. Seznam názvů připojení lze použít jako alternativu ke skupinám správců front k určení více připojení, která má klient vyzkoušet. Pokud konfigurujete správce front s více instancemi, můžete použít seznam názvů připojení k určení různých instancí správce front.

Pokud k definování kanálu mezi počítačem se systémem IBM MQ MQI client a počítačem se serverem použijete proměnnou prostředí **MQSERVER** , jedná se o jediný kanál, který je k dispozici pro vaši aplikaci, a na tabulku CCDT (Client Channel Definition Table) se neodkazuje.

Další informace naleznete v tématu Vytvoření kanálu připojení klienta v produktu IBM MQ MQI client using MQSERVER.

MQSNOAUT

Upozornění: Tato funkce se nedoporučuje.

Když nastavíte proměnnou prostředí **MQSNOAUT** na libovolnou hodnotu, zakáže správce oprávnění k objektu (OAM) a zabrání jakékoli kontrole zabezpečení. To může být vhodné pro testovací prostředí. To zahrnuje jak funkci autorizace, tak funkci ověření připojení. Zabezpečení TLS, záznamy ověřování kanálu a uživatelské procedury zabezpečení nejsou ovlivněny.

Proměnná prostředí **MQSNOAUT** se projeví pouze při vytvoření správce front.

Upozornění: Chcete-li povolit modul OAM, musíte odstranit správce front, odstranit proměnnou prostředí a poté znovu vytvořit správce front bez zadání parametru **MQSNOAUT**.

Další informace naleznete v tématu Prevence kontrol přístupu k zabezpečení na systémech AIX, Linuxa Windows.

MQSPREFIX

Jako alternativu ke změně výchozí předpony můžete použít proměnnou prostředí **MQSPREFIX** k přepsání proměnné **DefaultPrefix** pro příkaz **crtmqm** .

Další informace viz IBM MQ názvy souborů a sekce AllQueueManagers v souboru mqs.ini.

MQSSLCRYP

ALW

Proměnná prostředí **MQSSLCRYP** obsahuje řetězec parametrů, který můžete použít ke konfiguraci šifrovacího hardwaru přítomného v systému.

V 9.3.0 Povolené hodnoty jsou stejné jako pro pole SSLCryptoHardware v sekci SSL konfiguračního souboru klienta.

Chcete-li nastavit **MQSSLCRYP**, použijte jeden z těchto příkazů:

- Linux AIX Na systémech AIX and Linux:

```
export MQSSLCRYP=string
```

- Windows Na systémech Windows:

```
SET MQSSLCRYP=string
```

Další informace naleznete v tématu Konfigurace šifrovacího hardwaru na systémech AIX, Linux, and Windows a IBM MQ clients , které používají šifrovací hardware v tématu Ochrana hesel v IBM MQ konfiguračních souborech komponenty.

MQSSLFIPS

Proměnná prostředí **MQSSLFIPS** uvádí, zda se mají použít pouze algoritmy certifikované FIPS, pokud se šifrování provádí v produktu IBM MQ. Tuto proměnnou prostředí můžete nastavit na hodnotu YES nebo NO . Výchozí hodnota je NO. Tyto hodnoty jsou stejné jako pro parametr **SSLFIPS** příkazu **ALTER QMGR** .

Chcete-li nastavit **MQSSLFIPS**, použijte jeden z těchto příkazů:

- Linux AIX Na systémech AIX and Linux:

```
export MQSSLFIPS=YES|NO
```

- Windows Na systémech Windows:

```
SET MQSSLFIPS=YES|NO
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQSSLFIPS) VALUE(YES|NO)
```

Použití algoritmů s certifikací FIPS je ovlivněno použitím šifrovacího hardwaru. Další informace naleznete v tématu Určení, že se za běhu v klientu MQI používají pouze CipherSpecs s certifikací FIPS.

MQSSLKEYR

Proměnná prostředí **MQSSLKEYR** určuje umístění úložiště klíčů, které obsahuje digitální certifikát patřící uživateli.

V 9.3.0 V 9.3.0 Zadejte úplnou cestu a název souboru úložiště klíčů. Pokud není uvedena přípona souboru, předpokládá se, že je .kdb.

Chcete-li nastavit **MQSSLKEYR**, použijte jeden z těchto příkazů:

- Linux AIX Na systémech AIX and Linux:

```
export MQSSLKEYR=pathname
```

- Windows Na systémech Windows:

```
SET MQSSLKEYR=pathname
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQSSLKEYR) VALUE(pathname)
```

Pro tuto proměnnou prostředí neexistuje žádná výchozí hodnota.

Další informace viz parametr **SSLKEYR** příkazu **ALTER QMGR** .

MQSSLPROXY

Proměnná prostředí **MQSSLPROXY** určuje název hostitele a číslo portu serveru proxy HTTP, který má produkt GSKit používat pro kontroly OCSP.

Chcete-li nastavit **MQSSLPROXY**, použijte jeden z těchto příkazů:

- Linux AIX Na systémech AIX and Linux:

```
export MQSSLPROXY="string"
```

- Windows Na systémech Windows:

```
SET MQSSLPROXY= string
```

Řetězec, který zadáte s parametrem **MQSSLPROXY** , může být buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má produkt 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.

Linux AIX Například na systémech AIX and Linux můžete použít jeden z následujících příkazů:

-
```
export MQSSLPROXY="proxy.example.com(80)"
```

-
```
export MQSSLPROXY="127.0.0.1"
```

Další informace naleznete v tématu Práce s protokolem OCSP (Online Certificate Status Protocol).

MQSSLRESET

Proměnná prostředí **MQSSLRESET** uvádí počet nešifrovaných bajtů odeslaných a přijatých kanálem TLS, než bude znovu vyjednán tajný klíč TLS. Lze ji nastavit na celé číslo v rozsahu 0 až 999 999 999 999. Výchozí hodnota je 0, což označuje, že tajné klíče nejsou nikdy znovu vyjednány. Pokud uvedete počet resetů tajného klíče TLS v rozsahu 1 bajt až 32 kB, kanály TLS použijí počet resetů tajného klíče 32 kB. Tento počet tajných resetů se má vyvarovat nadměrných resetů klíčů, které by se vyskytly pro malé hodnoty resetu tajných klíčů TLS.

Chcete-li nastavit **MQSSLRESET**, použijte jeden z těchto příkazů:

- Linux AIX Na systémech AIX and Linux:

```
export MQSSLRESET=integer
```

- Windows Na systémech Windows:

```
SET MQSSLRESET=integer
```

- IBM i V systému IBM i:

```
ADDENVVAR ENVVAR(MQSSLRESET) VALUE(integer)
```

Další informace viz Resetování tajných klíčů SSL a TLS.

MQSUITEB

ALW

Produkt IBM MQ můžete nakonfigurovat tak, aby fungoval v souladu se standardem NSA Suite B na platformách AIX, Linux, and Windows .

Proměnná prostředí **MQSUITEB** uvádí, zda se má použít šifrování vyhovující standardu Suite B. Pokud se má použít šifrování Suite B, můžete určit sílu šifrování nastavením parametru **MQSUITEB** na jednu z následujících hodnot:

- NONE
- 128_BIT, 192_BIT
- 128_BIT
- 192_BIT

Můžete zadat více hodnot pomocí seznamu odděleného čárkami. Použití hodnoty NONE s jakoukoli jinou hodnotou je neplatné.

Další informace viz Konfigurace IBM MQ pro sadu B.

MQTCPTIMEOUT

Proměnná prostředí **MQTCPTIMEOUT** určuje, jak dlouho produkt IBM MQ čeká na volání připojení TCP.

ODQ_MSG

Používáte-li obslužnou rutinu fronty nedoručených zpráv, která se liší od produktu **runmqdlq**, je zdroj ukázky amqsdlqk dispozici pro použití jako základ. Ukázka je podobná obslužné rutině nedoručených zpráv poskytnuté v rámci produktu, ale trasování a hlášení chyb se liší. Pomocí proměnné prostředí **ODQ_MSG** nastavte název souboru obsahujícího chybové a informační zprávy. Poskytnutý soubor se nazývá amqsdlq.msg.

Další informace viz Ukázka obslužné rutiny fronty nedoručených zpráv.

ODQ_TRACE

Používáte-li obslužnou rutinu fronty nedoručených zpráv, která se liší od produktu **runmqdlq**, je zdroj ukázky amqsdlqk dispozici pro použití jako základ. Ukázka je podobná obslužné rutině nedoručených zpráv poskytnuté v rámci produktu, ale trasování a hlášení chyb se liší. Chcete-li povolit trasování, nastavte proměnnou prostředí **ODQ_TRACE** na hodnotu YES nebo yes.

Další informace viz Ukázka obslužné rutiny fronty nedoručených zpráv.

WCF_TRACE_ON

Pro vlastní kanál WCF jsou k dispozici dvě různé metody trasování. Tyto dvě metody trasování jsou aktivovány buď nezávisle, nebo společně. Každá metoda vytváří vlastní trasovací soubor, takže když jsou aktivovány obě trasovací metody, vygenerují se dva trasovací výstupní soubory. Existují čtyři kombinace pro povolení a zakázání dvou různých metod trasování. Kromě těchto kombinací pro povolení trasování WCF lze trasování XMS .NET povolit pomocí proměnné prostředí **WCF_TRACE_ON** .

Další informace naleznete v tématu Trasování vlastního kanálu WCF pro produkt IBM MQ.

Domovský_adresář_WMQSOAP_

Proměnná prostředí **WMQSOAP_HOME** se používá při provádění dalších konfiguračních kroků po správné instalaci a konfiguraci hostitelského prostředí služby .NET SOAP přes JMS v produktu IBM MQ. Je přístupný z lokálního správce front.

Další informace viz Klient WCF pro službu .NET , jejímž hostitelem je IBM MQ sample , a Klient WCF pro službu Axis Java , jejímž hostitelem je IBM MQ sample.

XMS_TRACE_ON, XMS_TRACE_FILE_PATH, XMS_TRACE_FORMAT a XMS_TRACE_SPECIFICATION

Používáte-li produkt IBM MQ classes for XMS .NET Framework, můžete konfigurovat trasování z konfiguračního souboru aplikace i z proměnných prostředí XMS . Pokud používáte IBM MQ classes for XMS .NET (knihovny.NET Standard a .NET 6), musíte nakonfigurovat trasování z proměnných prostředí XMS . Trasování se obvykle používá pod vedením podpory IBM .

Chcete-li povolit a konfigurovat trasování pro aplikaci XMS .NET , nastavte před spuštěním aplikace následující proměnné prostředí:

XMS_TRACE_ON
Je-li nastavena proměnná prostředí **XMS_TRACE_ON** , je standardně povoleno veškeré trasování.

XMS_TRACE_FILE_PATH
Proměnná prostředí **XMS_TRACE_FILE_PATH** uvádí úplný název cesty k adresáři, do kterého se zapisují záznamy trasování a FFDC, pokud chcete, aby se tyto záznamy zapisovaly do alternativního umístění z aktuálního pracovního adresáře.

XMS_TRACE_FORMAT
Proměnná prostředí **XMS_TRACE_FORMAT** uvádí požadovaný formát trasování, který může být buď BASIC , nebo ADVANCED.

SPECIFIKACE_TRASOVÁNÍ XMS_TRACE_SPECIFICATION
Proměnná prostředí **XMS_TRACE_SPECIFICATION** potlačí nastavení trasování definovaná v části Trasovat konfigurační soubor aplikace. **XMS_TRACE_SPECIFICATION** platí pouze pro IBM MQ classes for XMS .NET Framework .

Další informace viz Trasování XMS .NET aplikací a Trasování XMS .NET aplikací používajících XMS proměnné prostředí.

Multi Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms

Úpravou informací v konfiguračních souborech (`.ini`) můžete změnit chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovoval potřebám vaší instalace. Můžete také změnit volby konfigurace pro IBM MQ MQI clients.

Informace o této úloze

Informace o konfiguraci produktu IBM MQ můžete změnit na úrovni uzlu nebo správce front změnou hodnot určených v sadě konfiguračních atributů (nebo parametrů), které řídí produkt IBM MQ.

Konfigurační soubor (nebo soubor sekcí) obsahuje jednu nebo více sekcí, což jsou skupiny řádků v souboru `.ini` , které mají společnou funkci nebo definují část systému, jako jsou funkce protokolu, funkce kanálu a instalovatelné služby. Atributy konfigurace IBM MQ můžete upravit v následujících konfiguračních souborech:

IBM MQ konfigurační soubor, `mqs.ini`
Soubor `mqs.ini` ovlivňuje změny v uzlu jako celku. Pro každou instalaci produktu IBM MQ existuje jeden soubor `mqs.ini` .

Vzhledem k tomu, že konfigurační soubor IBM MQ se používá k vyhledání dat přidružených ke správcům front, může neexistující nebo chybný konfigurační soubor způsobit selhání některých nebo všech příkazů MQSC. Aplikace se také nemohou připojit ke správci front, který není definován v konfiguračním souboru IBM MQ .

Konfigurační soubor instalace mqinst.ini
Linux AIX Na systémech AIX and Linux obsahuje konfigurační soubor instalace `mqinst.ini`informace o všech instalacích produktu IBM MQ . Soubor `mqinst.ini` nesmí být upraven nebo odkazován přímo, protože jeho formát není pevný a mohl by se změnit. Místo toho jej musíte upravit pomocí příkazů.

Konfigurační soubor správce front, `qm.ini`
Soubor `qm.ini` ovlivňuje změny pro specifické správce front. Pro každého správce front v uzlu existuje jeden soubor `qm.ini` .

IBM MQ MQI client konfigurační soubor mqclient.ini
Volby konfigurace pro IBM MQ MQI clients jsou drženy odděleně, v konfiguračním souboru klienta, který je obecně pojmenován `mqclient.ini`.

Konfigurační soubor trasování aktivity mqat.ini
Soubor `mqat.ini` se používá ke konfiguraci chování trasování aktivity.

Možná budete muset upravit konfigurační soubor, pokud například:

- Ztratíte konfigurační soubor. (Pokud můžete, obnovte jej ze zálohy.)
- Je třeba přesunout jednoho nebo více správců front do nového adresáře.
- Je třeba změnit výchozího správce front. K tomu může dojít, pokud omylem odstraníte existujícího správce front.
- Doporučuje se, abyste tak činili prostřednictvím podpory IBM .

Důležité: Změny, které provedete v konfiguračním souboru, se obvykle projeví až při příštím spuštění správce front.

Poznámky k úpravám konfiguračních souborů:

- Hodnoty atributů 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` .
- Po instalaci můžete upravit výchozí hodnoty v konfiguračních souborech IBM MQ .
- Při zálohování správce front nezapomeňte zahrnout jak jeho konfigurační soubor (`qm.ini`), tak i centrální konfigurační soubor IBM MQ (`mqs.ini`).
- Nastavíte-li nesprávnou hodnotu atributu konfiguračního souboru, efekt bude stejný, jako kdyby atribut zcela chyběl. Hodnota je ignorována a je vydána zpráva operátora, která označuje problém.
- IBM i V systému IBM ijsou soubory `.ini` proudové soubory rezidentní v IFS.
- Existuje řada pravidel syntaxe pro formát souboru `mqat.ini` . Další informace naleznete v tématu Trasování aktivity aplikace Konfigurace chování trasování aktivity pomocí produktu `mqat.ini`.

Postup

1. Před úpravou konfiguračního souboru jej zazálohujte, abyste měli kopii, ke které se můžete vrátit, pokud to bude potřeba.
2. Upravte konfigurační soubor `.ini` jedním z následujících způsobů:
   - Ručně pomocí standardního textového editoru. Komentáře lze zahrnout do konfiguračních souborů přidáním znaku ";" nebo "#" před text komentáře. Chcete-li použít znak ";" nebo "#" bez toho, aby představoval komentář, můžete před něj přidat znak "\" . Znak se pak použije jako součást konfiguračních dat.
   - Automaticky pomocí příkazů, které mění konfiguraci správců front v uzlu. Další informace viz Popis příkazů.

     Windows Například Windows specifický příkaz **amqmdain** automaticky aktualizuje podmnožinu vlastností `qm.ini` . Další informace viz amqmdain.
   - Windows Linux V systémech Linux (x86 a x86-64) a Windowsmůžete aktualizovat podmnožinu vlastností `qm.ini` pomocí IBM MQ Explorer. Další informace naleznete v tématu Konfigurace produktu IBM MQ pomocí produktu MQ Explorer.

Poznámka: Vzhledem k tomu, že změny instalovatelných služeb a jejich komponent mají významné důsledky, jsou instalovatelné služby v produktu IBM MQ Explorerjen pro čtení. Proto musíte provést jakékoli změny instalovatelných služeb úpravou souboru `qm.ini` . Další informace viz téma “Sekce služby souboru qm.ini” na stránce 139.

Související úlohy

Správa serveruIBM MQ

Multi IBM MQ konfigurační soubor mqs.ini

Konfigurační soubor IBM MQ `mqs.ini`obsahuje informace důležité pro všechny správce front v uzlu. Vytvoří se automaticky během instalace.

Poznámka: Další informace o tom, jak a kdy upravit soubor `mqs.ini` a kdy se projeví změny provedené v souboru, viz “Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83.

Umístění adresářů

Linux AIX V systému AIX and Linuxjsou datový adresář a adresář protokolu vždy `/var/mqm` a `/var/mqm/log` .

Windows Na systémech Windows je umístění datového adresáře `mqs.ini`a umístění adresáře protokolu uloženo v registru, protože jejich umístění se může lišit. Informace o konfiguraci instalace, které jsou obsaženy v produktu `mqinst.ini` na systémech AIX and Linux , jsou také v registru, protože v systému Windows není žádný soubor `mqinst.ini` (viz “Konfigurační soubor instalace mqinst.ini” na stránce 154).

Windows Soubor `mqs.ini` pro systémy Windows je dán WorkPath uvedenou v klíči `HKLM\SOFTWARE\IBM\IBM MQ` . Obsahuje:

- Názvy správců front
- Název výchozího správce front
- Umístění souborů přidružených ke každému z nich

IBM i V systému IBM ije soubor `mqs.ini` uložen v adresáři `/QIBM/UserData/mqm`. Soubor obsahuje:

- Názvy správců front.
- Název výchozího správce front.
- Umístění souborů přidružených ke každému správci front.
- Informace identifikující všechny uživatelské procedury rozhraní API (další informace viz Konfigurace uživatelských procedur rozhraní API).

Soubor `mqs.ini` se používá zejména k vyhledání dat přidružených k jednotlivým správcům front.

Příklad souboru `mqs.ini` pro AIX and Linux

Linux AIX

```
#*******************************************************************#
#* Module Name: mqs.ini                                            *#
#* Type       : IBM MQ Machine-wide Configuration File             *#
#* Function   : Define IBM MQ resources for an entire machine      *#
#*******************************************************************#
#* Notes      :                                                    *#
#* 1) This is the installation time default configuration          *#
#*                                                                 *#
#*******************************************************************#
AllQueueManagers:
#*******************************************************************#
```

```
#* The path to the qmgrs directory, below which queue manager data     *#
#* is stored                                                           *#
#*********************************************************************#
DefaultPrefix=/var/mqm

LogDefaults:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0
   LogDefaultPath=/var/mqm/log

QueueManager:
   Name=saturn.queue.manager
   Prefix=/var/mqm
   Directory=saturn!queue!manager
   InstallationName=Installation1

QueueManager:
   Name=pluto.queue.manager
   Prefix=/var/mqm
   Directory=pluto!queue!manager
   InstallationName=Installation2

DefaultQueueManager:
   Name=saturn.queue.manager

ApiExitTemplate:
   Name=OurPayrollQueueAuditor
   Sequence=2
   Function=EntryPoint
   Module=/usr/ABC/auditor
   Data=123

ApiExitCommon:
   Name=MQPoliceman
   Sequence=1
   Function=EntryPoint
   Module=/usr/MQPolice/tmqp
   Data=CheckEverything
```

Příklad souboru `mqs.ini` pro Windows

Windows

```
#*********************************************************************#
#* Module Name: mqs.ini                                              *#
#* Type       : IBM MQ Machine-wide Configuration File               *#
#* Function   : Define IBM MQ resources for an entire machine        *#
#*********************************************************************#
#* Notes      :                                                      *#
#* 1) This is the installation time default configuration            *#
#*                                                                   *#
#*********************************************************************#
AllQueueManagers:
#*********************************************************************#
#* The path to the qmgrs directory, below which queue manager data     *#
#* is stored                                                           *#
#*********************************************************************#
DefaultPrefix=C:\ProgramData\IBM\MQ

LogDefaults:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0
   LogDefaultPath=C:\ProgramData\IBM\MQ\log

QueueManager:
   Name=saturn.queue.manager
   Prefix=C:\ProgramData\IBM\MQ
   Directory=saturn!queue!manager
   InstallationName=Installation1

QueueManager:
   Name=pluto.queue.manager
```

```
   Prefix=C:\ProgramData\IBM\MQ
   Directory=pluto!queue!manager
   InstallationName=Installation2

DefaultQueueManager:
   Name=saturn.queue.manager

ApiExitTemplate:
   Name=OurPayrollQueueAuditor
   Sequence=2
   Function=EntryPoint
   Module=C:\usr\ABC\auditor
   Data=123

ApiExitCommon:
   Name=MQPoliceman
   Sequence=1
   Function=EntryPoint
   Module=C:\usr\MQPolice\tmpq
   Data=CheckEverything
```

Příklad souboru `mqs.ini` pro IBM i


```
#*******************************************************************#
#* Module Name: mqs.ini                                            *#
#* Type       : IBM MQ Configuration File                          *#
#* Function   : Define IBM MQ resources for the node               *#
#*                                                                 *#
#*******************************************************************#
#* Notes      :                                                    *#
#* 1) This is an example IBM MQ configuration file                 *#
#*                                                                 *#
#*******************************************************************#
AllQueueManagers:
#*******************************************************************#
#* The path to the qmgrs directory, within which queue manager data*#
#* is stored                                                       *#
#*******************************************************************#
DefaultPrefix=/QIBM/UserData/mqm

QueueManager:
Name=saturn.queue.manager
Prefix=/QIBM/UserData/mqm
Library=QMSATURN.Q
Directory=saturn!queue!manager

QueueManager:
Name=pluto.queue.manager
Prefix=/QIBM/UserData/mqm
Library=QMPLUTO.QU
Directory=pluto!queue!manager

DefaultQueueManager:
Name=saturn.queue.manager
```

Notes:

1. Produkt IBM MQ v uzlu používá výchozí umístění pro správce front a žurnály.
2. Správce front saturn.queue.manager je výchozím správcem front pro daný uzel. Adresář pro soubory přidružené k tomuto správci front byl automaticky převeden na platný název souboru pro systém souborů.
3. Vzhledem k tomu, že konfigurační soubor IBM MQ se používá k vyhledání dat přidružených ke správcům front, může neexistující nebo chybný konfigurační soubor způsobit selhání některých nebo všech příkazů IBM MQ . Aplikace se také nemohou připojit ke správci front, který není definován v konfiguračním souboru IBM MQ .

`mqs.ini` sekcí

Upozornění: Toto téma odkazuje na další informace o oddílech v souboru `mqs.ini` . Každá sekce obsahuje informace o parametrech v této sekci.

Multi Souhrn sekcí a atributů souboru mqs.ini

Souhrn atributů sekcí konfiguračního souboru IBM MQ `mqs.ini`s odkazy na další informace.

Tabulka 9. Sekce souboru mqs.ini

Sekce a atributy	Popis atributů
AllQueueSekce správců	
DefaultPrefix	Cesta k adresáři `qmgrs` , v němž jsou uchovávána data správce front.
ALW DefaultEphemeralPředpona	Cesta k adresáři, v němž jsou uchovávána dočasná data správce front.
Multi ConvEBCDICNewline	Jak IBM MQ převádí znak NL EBCDIC na formát ASCII
ApiExitSpolečná sekce a ApiExitSekce šablony	
Název	Popisný název uživatelské procedury rozhraní API, která jí byla předána v poli ExitInfoNázev struktury MQAXP.
funkce	Název vstupního bodu funkce do modulu obsahujícího kód uživatelské procedury rozhraní API.
Modul	Modul obsahující kód uživatelské procedury rozhraní API.
Data	Data, která mají být předána uživatelské proceduře rozhraní API v poli ExitData struktury MQAXP.
Posloupnost	Posloupnost, ve které je tato uživatelská procedura rozhraní API volána vzhledem k jiným uživatelským procedurám rozhraní API.
DefaultQueueSekce správce	
Název	Název správce front, který zpracovává všechny příkazy, pro které není explicitně určen název správce front.
ExitProperties stanza	
CLWLMode	Zda uživatelská procedura CLWL (cluster workloac) běží buď v režimu FAST, nebo v režimu SAFE.
LogDefaults stanza	
LogPrimaryFiles	Soubory protokolu přidělené při vytvoření správce front.
LogSecondaryFiles	Soubory protokolu přidělené při vyčerpání primárních souborů.
LogFilePages	Počet stránek souboru protokolu. (Velikost souboru protokolu je určena v jednotkách stránek o velikosti 4 kB.)
LogType	Typ protokolování, které má použít správce front (kruhové nebo lineární).
LogBufferPages	Množství paměti přidělené záznamům vyrovnávací paměti pro zápis, určující velikost vyrovnávacích pamětí v jednotkách 4kB stránek.

Tabulka 9. Sekce souboru mqs.ini (pokračování)	
Sekce a atributy	**Popis atributů**
LogDefaultPath	Adresář, ve kterém jsou umístěny soubory protokolu pro správce front.
LogWriteIntegrity	Metoda, kterou modul protokolování používá k spolehlivému zápisu záznamů protokolu.
QueueManager	
Název	Název správce front.
Předpona	Kde jsou uloženy soubory správce front.
Adresář	Název podadresáře v adresáři `prefix\QMGRS` , kde jsou uloženy soubory správce front.
DataPath	Explicitní cesta k datům poskytnutá při vytvoření správce front přepíše předponu a adresář jako cestu k datům správce front.
InstallationName	Název instalace produktu IBM MQ přidružené k tomuto správci front.
EphemeralPrefix	Kde jsou uložena dočasná data správce front.

Multi AllQueueSekce správců souboru mqs.ini

Sekce AllQueueManagers může určit cestu k adresáři `qmgrs` , kde jsou uloženy soubory přidružené ke správci front, cestu ke spustitelné knihovně a metodu pro převod dat ve formátu EBCDIC na formát ASCII.

Pomocí sekce AllQueueManagers v souboru `mqs.ini` zadejte informace o všech správcích front.

Windows Linux Případně na systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `General` a `Extended` IBM MQ .

DefaultPrefix= ***název_adresáře***
Tento atribut určuje cestu k adresáři `qmgrs` , v němž jsou uchovávána data správce front.

Změníte-li výchozí předponu pro správce front, replikujte adresářovou strukturu, která byla vytvořena v době instalace. Zejména musíte vytvořit strukturu qmgrs. Zastavte IBM MQ před změnou výchozí předpony a restartujte IBM MQ pouze poté, co jste přesunuli struktury do nového umístění a změnili výchozí předponu.

Poznámka: ALW Neodstraňujte adresář `/var/mqm/errors` na systémech AIX and Linux ani adresář `\errors` na systémech Windows .

Jako alternativu ke změně výchozí předpony můžete použít proměnnou prostředí **MQSPREFIX** k přepsání **DefaultPrefix** pro příkaz **crtmqm** .

Vzhledem k omezením operačního systému ponechte zadanou cestu dostatečně krátkou, aby součet délky cesty a libovolného názvu správce front byl maximálně 70 znaků dlouhý.

Multi **DefaultEphemeralPředpona =** ***název_adresáře***
Tento atribut určuje cestu k adresáři, v němž jsou uchovávána dočasná data správce front, například sokety IPC, a používá se pouze k nastavení **EphemeralPrefix** správce front při vytvoření správce front. Kromě toho musíte adresář vytvořit sami, pokud změníte výchozí hodnotu. Musíte vytvořit dočasný datový adresář s oprávněními, která umožní skupině IBM MQ přístup k zápisu do tohoto adresáře.

Jako alternativu ke změně souboru `mqs.ini` můžete použít proměnnou prostředí **MQ_EPHEMERAL_PREFIX** k přepsání **DefaultEphemeralPrefix** pro příkaz **crtmqm** .

Kvůli omezením operačního systému je výchozí efemérní předpona omezena na:

- Linux AIX 12 znaků na platformách AIX and Linux .
- IBM i 24 znaků na IBM i.

MQ Appliance **DefaultEphemeralPrefix** není na serveru IBM MQ Appliancepodporován.

Multi **ConvEBCDICNewline= NL_TO_LF | TABLE | ISO**
Kódové stránky EBCDIC obsahují znak nového řádku (NL), který není podporován kódovými stránkami ASCII (ačkoli některé varianty ISO ASCII obsahují ekvivalent). Pomocí atributu **ConvEBCDICNewline** určete, jak má IBM MQ převést znak NL EBCDIC na formát ASCII.

IBM i V systému IBM MQ for IBM ije CCSID 1253 považován za ISO CCSID a NL_TO_LF ovlivňuje převody ISO i ASCII.

z/OS Atribut **ConvEBCDICNewline** není k dispozici na systému z/OS. Chování v systému z/OS je ekvivalentní ConvEBCDICNewline=TABLE. Všimněte si, že výchozí nastavení na jiných platformách se může lišit.

NL_TO_LF
Převeďte znak NL EBCDIC (X'15 ') na znak LF (X'0A') ASCII pro všechny převody EBCDIC na ASCII.

NL_TO_LF je předvolba.

TABULKA
Převeďte znak NL EBCDIC podle převodních tabulek použitých na vaší platformě pro všechny konverze EBCDIC na ASCII.

Účinek tohoto typu převodu se může lišit od platformy k platformě a od jazyka k jazyku; i na stejné platformě se může chování lišit, pokud používáte různé CCSID.

ISO
Převést:

- ISO CCSID používající metodu TABLE
- Všechny ostatní CCSID používající metodu NL_TO_CF

Možné ISO CCSID jsou uvedeny v souboru Tabulka 10 na stránce 90.

Tabulka 10. 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

Pokud ASCII CCSID není podmnožina ISO, **ConvEBCDICNewline** standardně zobrazuje NL_TO_LF.

V systémech IBM MQ 9.1.0 Fix Pack 2 a IBM MQ 9.1.2můžete použít atribut proměnná prostředí **AMQ_CONVEBCDICNEWLINE** místo atributu sekce **ConvEBCDICNewline** , například k poskytnutí funkčnosti **ConvEBCDICNewline** na straně klienta v situacích, kdy nelze použít

soubor `mqs.ini` . Proměnná prostředí má stejné hodnoty (`NL_TO_LF`, `TABLE`nebo `ISO`) jako atribut **ConvEBCDICNewline** . Atribut stanza má přednost, pokud je nastaven atribut i proměnná prostředí.

Multi ApiExitCommon a ApiExitstanzas šablony souboru mqs.ini

Sekce ApiExitTemplate a ApiExitCommon identifikují uživatelské procedury rozhraní API pro všechny správce front.

Pomocí šablony ApiExita společných sekcí ApiExitv souboru `mqs.ini` identifikujte uživatelské procedury rozhraní API pro všechny správce front. (Chcete-li identifikovat uživatelské procedury rozhraní API pro jednotlivé správce front, použijte lokální sekci ApiExit, jak je popsáno v tématu “ApiExitLokální sekce souboru qm.ini” na stránce 109.)

Windows Linux Případně na systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `Exits` IBM MQ .

Windows V systému Windowsmůžete také pomocí příkazu **amqmdain** změnit položky pro uživatelské procedury rozhraní API.

Další informace o použití těchto atributů naleznete v tématu Konfigurace uživatelských procedur rozhraní API.

Název = ApiExit_name
Popisný název uživatelské procedury rozhraní API, která jí byla předána v poli ExitInfoNázev struktury MQAXP.

Tento název musí být jedinečný, nesmí být delší než 48 znaků a musí obsahovat pouze platné znaky pro názvy objektů IBM MQ (například názvy front).

Funkce=název_funkce
Název vstupního bodu funkce do modulu obsahujícího kód uživatelské procedury rozhraní API. Tento vstupní bod je funkcí MQ_INIT_EXIT.

Délka pole je omezena hodnotou MQ_EXIT_NAME_LENGTH.

Module=název_modulu
Modul obsahující kód uživatelské procedury rozhraní API.

Pokud pole obsahuje název modulu včetně úplné cesty, je použit beze změny. Pokud toto pole obsahuje pouze název modulu, je modul umístěn pomocí atributu **ExitsDefaultPath** v sekci `ExitPath` souboru `qm.ini` .

Na platformách, které podporují samostatné knihovny s podporou podprocesů, musíte poskytnout verzi modulu uživatelské procedury rozhraní API bez podpory podprocesů i s podporou podprocesů. Verze s podprocesy musí mít příponu `_r` . Verze se podprocesy stubu aplikace IBM MQ implicitně připojí `_r` k danému názvu modulu před jeho načtením.

Délka tohoto pole je omezena na maximální délku cesty, kterou platforma podporuje.

Data=název_dat
Data, která mají být předána uživatelské proceduře rozhraní API v poli ExitData struktury MQAXP.

Pokud zahrnete tento atribut, počáteční a koncové mezery se odeberou, zbývající řetězec se ořízne na 32 znaků a výsledek se předá uživatelské proceduře. Vynecháte-li tento atribut, přednastavená hodnota 32 mezer se předá uživatelské proceduře.

Maximální délka tohoto pole je 32 znaků.

Sekvence=pořadové_číslo
Posloupnost, ve které je tato uživatelská procedura rozhraní API volána vzhledem k jiným uživatelským procedurám rozhraní API. Ukončení s nízkým pořadovým číslem je voláno před ukončením s vyšším pořadovým číslem. Není třeba, aby pořadové číslování východů bylo souvislé. Posloupnost 1, 2, 3 má stejný výsledek jako posloupnost 7, 42, 1096. Pokud mají dvě uživatelské procedury stejné pořadové číslo, rozhodne se správce front, která z nich má být volala jako první. Můžete určit, který byl volán po události, vložením času nebo značkovače do oblasti ExitChainoznačené ExitChainAreaPtr v MQAXP nebo zápisem vlastního souboru protokolu.

Tento atribut je číselná hodnota bez znaménka.

Multi DefaultQueueSekce správce souboru mqs.ini

Sekce DefaultQueueManager určuje výchozího správce front pro uzel.

Pomocí sekce DefaultQueueManager v souboru `mqs.ini` určete výchozího správce front.

Windows Linux Případně na systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `General` IBM MQ .

Název = *default_queue_manager*
Výchozí správce front zpracovává všechny příkazy, pro které není explicitně zadán název správce front. Atribut **`DefaultQueueManager`** se automaticky aktualizuje, pokud vytvoříte nového výchozího správce front. Pokud neúmyslně vytvoříte nového výchozího správce front a poté se chcete vrátit k původnímu, změňte atribut **`DefaultQueueManager`** ručně.

Multi ExitProperties sekce souboru mqs.ini

Sekce ExitProperties určuje volby konfigurace používané programy uživatelských procedur správce front.

Sekci ExitProperties v souboru `mqs.ini` použijte k určení voleb konfigurace, které používají uživatelské programy správce front.

Windows Linux Případně na systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `Extended` IBM MQ .

CLWLMode = SAFE (výchozí) | RYCHLE
Uživatelská procedura pracovní zátěže klastru (CLWL) vám umožňuje určit, která fronta klastru se má v klastru otevřít v reakci na volání MQI (například `MQOPEN`, `MQPUT`). Uživatelská procedura CLWL se spustí buď v režimu FAST, nebo v režimu SAFE v závislosti na hodnotě zadané v atributu **`CLWLMode`** . Pokud vynecháte atribut **`CLWLMode`** , uživatelská procedura pracovní zátěže klastru se spustí v režimu SAFE.

Bezpečný
Spusťte uživatelskou proceduru CLWL v odděleném procesu od správce front. Toto nastavení je výchozí.

Pokud při spuštění v režimu SAFE dojde k problému s uživatelskou procedurou CLWL, dojde k následujícím událostem:

- Proces serveru CLWL (amqzlwa0) selže.
- Správce front restartuje proces serveru CLWL.
- Chyba je vám nahlášena v protokolu chyb. Pokud probíhá volání MQI, obdržíte oznámení ve formě návratového kódu.

Integrita správce front je zachována.

Poznámka: Spuštění uživatelské procedury CLWL v samostatném 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 procesů přidruženým ke spuštění v režimu SAFE, ale učiníte tak na úkor integrity správce front. Uživatelskou proceduru CLWL byste měli spustit pouze v režimu FAST, pokud jste přesvědčeni, že s uživatelskou procedurou CLWL nejsou žádné problémy, a jste obzvláště znepokojeni výkonem.

Pokud dojde k problému při spuštění uživatelské procedury CLWL v režimu FAST, dojde k selhání správce front a riskujete ohrožení integrity správce front.

Multi Sekce LogDefaults souboru mqs.ini

Sekce LogDefaults uvádí informace o předvolbách protokolu pro všechny správce front.

Sekci LogDefaults v souboru `mqs.ini` použijte k uvedení informací o předvolbách protokolu pro všechny správce front.

Windows Linux Případně na systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `Default log settings` IBM MQ .

Pokud požadujete jinou než výchozí hodnotu, musíte tuto hodnotu explicitně uvést v sekci LogDefaults .

Pokud sekce LogDefaults neexistuje, pak se použijí předvolby IBM MQ . Atributy protokolu se používají jako výchozí hodnoty při vytváření správce front, ale lze je přepsat, pokud zadáte atributy protokolu v příkazu **crtmqm** . Další informace o tomto příkazu viz **crtmqm**.

Po vytvoření správce front jsou atributy protokolu pro tohoto správce front převzaty z nastavení popsaných v tématu “Sekce protokolu souboru qm.ini” na stránce 130.

Poznámka: Dodaná sekce LogDefaults pro novou instalaci IBM MQ neobsahuje žádné explicitní hodnoty pro atributy. Nedostatek atributu znamená, že výchozí hodnota pro tuto hodnotu se použije při vytvoření nového správce front. Výchozí hodnoty pro sekci LogDefaults jsou zobrazeny v “Příklad souboru mqs.ini pro AIX and Linux” na stránce 85 a “Příklad souboru mqs.ini pro Windows” na stránce 86. Hodnota nula pro atribut `LogBufferPages` znamená 512.

Výchozí předpona, která je určena v souboru “AllQueueSekce správců souboru mqs.ini” na stránce 89, a cesta k protokolu určená pro konkrétního správce front, která je určena v souboru “Sekce protokolu souboru qm.ini” na stránce 130, umožňují správci front a jeho protokolu být na různých fyzických jednotkách. Jedná se o doporučenou metodu, i když jsou standardně na stejné jednotce.

Informace o výpočtu velikosti protokolu viz “Výpočet velikosti protokolu” na stránce 628.

Poznámka: Limity uvedené v následujícím seznamu parametrů jsou limity nastavené parametrem IBM MQ. Omezení operačního systému mohou snížit maximální možnou velikost protokolu.

LogPrimaryFiles = 3 (výchozí) |*2-254* (Windows) |*2-510* (AIX and Linux)
Soubory protokolu přidělené při vytvoření správce front.

Minimální počet primárních souborů protokolu, které můžete mít, je 2 a maximální počet je 254 v systému Windowsnebo 510 v systému AIX and Linux. Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systému AIX and Linuxa nesmí být menší než 3.

Hodnota je ověřována při vytváření nebo spouštění správce front. Po vytvoření správce front jej můžete změnit. Změna hodnoty se však neprojeví, dokud nebude správce front restartován a efekt nemusí být okamžitý.

LogSecondaryFiles = 2 (výchozí) |*1-253* (Windows) |*1-509* (AIX and Linux)
Soubory protokolu přidělené při vyčerpání primárních souborů.

Minimální počet sekundárních souborů protokolu je 1 a maximum je 253 v systému Windowsnebo 509 v systému AIX and Linux. Výchozí číslo je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systému AIX and Linuxa nesmí být menší než 3.

Hodnota je prozkoumána při spuštění správce front. Tuto hodnotu můžete změnit, ale změny se neprojeví, dokud nebude správce front restartován, a i tak nemusí být efekt okamžitý.

LogFilePočet stránek = *number*
Data protokolu jsou uložena v řadě souborů nazývaných soubory protokolu. Velikost souboru protokolu je určena v jednotkách stránek o velikosti 4 kB.

Výchozí počet stránek souboru protokolu je 4096 a velikost souboru protokolu je 16 MB.

V systému AIX and Linuxje minimální počet stránek souboru protokolu 64 a v systému Windowsje minimální počet stránek souboru protokolu 32; v obou případech je maximální počet 65 535.

Poznámka: Velikost souborů protokolu určenou při vytváření správce front nelze pro správce front změnit.

LogType = CIRCULAR (výchozí) | LINEAR
Typ protokolu, který se má použít. Výchozí hodnota je CIRCULAR.

KRUHOVÉ
Spusťte obnovu po restartu pomocí protokolu, abyste odvolali transakce, které probíhaly, když byl systém zastaven.

Podrobnější vysvětlení kruhového protokolování naleznete v části “Typy protokolování” na stránce 623 .

Lineární
Jak pro obnovu po restartu, tak pro obnovu po předání (vytváření ztracených nebo poškozených dat přehráváním obsahu protokolu).

Podrobnější vysvětlení lineárního protokolování naleznete v části “Typy protokolování” na stránce 623 .

Chcete-li změnit předvolbu, můžete buď upravit atribut LogType , nebo zadat lineární protokolování pomocí příkazu **crtmqm** .

V produktu IBM MQ 9.1.0můžete změnit metodu protokolování po vytvoření správce front. Další informace viz migmqlog.

LogBufferPages=0 (výchozí) |*0-4096*
Množství paměti přidělené záznamům vyrovnávací paměti pro zápis, určující velikost vyrovnávacích pamětí v jednotkách 4kB stránek.

Minimální počet stránek vyrovnávací paměti je 18 a maximální je 4096. Větší vyrovnávací paměti přispívají k vyšší propustnosti, zvláště velkých zpráv.

Zadáte-li hodnotu 0 (výchozí hodnota), správce front vybere velikost 512 (2048 kB).

Zadáte-li číslo v rozsahu 1 až 17, bude pro správce front použita výchozí hodnota 18 (72 kB). Zadáte-li číslo v rozsahu 18 až 4096, použije správce front zadané číslo k nastavení přidělené paměti.

LogDefaultCesta = *název_adresáře*
Adresář, ve kterém jsou umístěny soubory protokolu pro správce front. Adresář je umístěn na lokálním zařízení, do kterého může správce front zapisovat, a pokud možno na jiné jednotce než ve frontách zpráv. Uvedení jiné jednotky poskytuje přidanou ochranu v případě selhání systému.

Výchozí nastavení je:

- Windows *DefaultPrefix*\log pro IBM MQ for Windows , kde *DefaultPrefix* je hodnota uvedená v atributu DefaultPrefix na stránce vlastností All Queue Managers IBM MQ . Tato hodnota je nastavena v době instalace.
- Linux AIX /var/mqm/log pro systémy AIX and Linux .

Případně můžete zadat název adresáře v příkazu **crtmqm** pomocí příznaku **-ld** . Při vytvoření správce front je v adresáři správce front vytvořen také adresář, který slouží k uchování souborů protokolu. Název tohoto adresáře je založen na názvu správce front. Tím zajistíte, že cesta k souboru protokolu bude jedinečná a že bude v souladu se všemi omezeními délky názvů adresářů.

Pokud neuvedete **-ld** v příkazu **crtmqm** , použije se hodnota atributu **LogDefaultPath** v souboru mqs.ini .

Název správce front se připojí k názvu adresáře, aby se zajistilo, že více správců front bude používat různé adresáře protokolu.

Při vytvoření správce front je v atributech protokolu v informacích o konfiguraci vytvořena hodnota **LogPath** s uvedením úplného názvu adresáře pro protokol správce front. Tato hodnota se používá k vyhledání protokolu při spuštění nebo odstranění správce front.

LogWriteIntegrity =SingleWrite|DoubleWrite|TripleWrite (výchozí)
Metoda, kterou modul protokolování používá k spolehlivému zápisu záznamů protokolu.

TripleWrite (výchozí)

Všimněte si, že lze vybrat volbu DoubleWrite. Když tak ale uděláte, systém to interpretuje jako volbu TripleWrite.

SingleWrite
Měli byste použít SingleWrite, pouze pokud systém souborů a zařízení hostující protokol pro zotavení IBM MQ výslovně zaručují atomicitu 4KB zápisů.

Když se tedy zápis 4kB stránky nezdaří z nějakého důvodu, jsou možné jen dva stavy: před obrazem nebo po obrazu. Žádný mezistav by neměl být možný.

Poznámka: Pokud je ve vaší trvalé pracovní zátěži dostatečná souběžnost, existuje minimální potenciální přínos při nastavování jiné než výchozí hodnoty TripleWrite.

Další informace viz téma "LogWriteIntegrita-použití SingleWrite nebo TripleWrite" na stránce 133.

Multi QueueManager sekce souboru mqs.ini

Sekce QueueManager určuje umístění adresáře správce front.

Pro každého správce front existuje jedna sekce QueueManager . Atributy této sekce určují název správce front a název adresáře obsahujícího soubory přidružené k tomuto správci front. Název adresáře je založen na názvu správce front, ale je transformován, pokud název správce front není platný název souboru. Další informace o transformaci názvů naleznete v tématu Základní informace o IBM MQ názvech souborů.

Název = *název_správce_fronty*
Název správce front.

Prefix = *prefix*
Kde jsou uloženy soubory správce front. Standardně je tato hodnota stejná jako hodnota uvedená v atributu **DefaultPrefix** sekce Všichni správci front v souboru mqs.ini .

Adresář = *název*
Název podadresáře v adresáři *prefix*\QMGRS , kde jsou uloženy soubory správce front. Tento název je založen na názvu správce front, ale může být transformován, pokud existuje duplicitní název nebo pokud název správce front není platný název souboru.

DataPath= *cesta*
Explicitní cesta k datům poskytnutá při vytvoření správce front přepíše **Prefix** a **Directory** jako cestu k datům správce front.

InstallationName= *název*
Název instalace produktu IBM MQ přidružené k tomuto správci front. Při interakci s tímto správcem front musí být použity příkazy z této instalace.

IBM i **Knihovna = *název***
Název knihovny, kde jsou uloženy objekty IBM i , které se vztahují k tomuto správci front, například žurnály a žurnálové zásobníky. Tento název je založen na názvu správce front, ale může být transformován, pokud existuje duplicitní název nebo pokud název správce front není platný název knihovny.

EphemeralPrefix= *název*
Kde jsou uložena dočasná data správce front.

Standardně tato hodnota není přítomna, což znamená, že data jsou uložena v umístění Předpona.

Hodnota je nastavena z hodnoty proměnné prostředí **MQ_EPHEMERAL_PREFIX** nebo atributu **DefaultEphemeralPrefix** sekce AllQueueManagers v souboru mqs.ini při vytvoření správce front.

IBM i Kvůli omezením operačního systému je výchozí efemérní předpona v systému IBM iomezena na 24 znaků.

Související úlohy

“Přidružení správce front k instalaci” na stránce 451

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

Windows Rozhraní ACPI (Advanced Configuration and Power Interface)

Produkt Windows podporuje standard ACPI (Advanced Configuration and Power Interface). To umožňuje uživatelům systému Windows s hardwarem s povoleným ACPI zastavit a restartovat kanály, když systém vstoupí do režimu pozastavení a pokračuje v režimu pozastavení.

Na stránce vlastností produktu ACPI IBM MQ z adresáře IBM MQ Explorer můžete určit, jak se má produkt IBM MQ chovat, když systém obdrží požadavek na pozastavení.

Všimněte si, že nastavení uvedená na stránce vlastností produktu ACPI IBM MQ se použijí pouze v případě, že je spuštěn monitor výstrah. Ikona Monitor výstrah je na hlavním panelu přítomna, pokud je monitor výstrah spuštěn.

DoDialog= Y | N
Zobrazí dialogové okno v době požadavku na pozastavení.

DenySuspend= Y | N
Zamítne požadavek na pozastavení. Používá se, pokud DoDialog= N, nebo pokud DoDialog= Y a dialogové okno nelze zobrazit, například proto, že je vaše víko zápisníku zavřené.

CheckChannelsRunning=Y | N
Zkontroluje, zda jsou spuštěny nějaké kanály. Výsledek může určit výsledek ostatních nastavení.

Následující tabulka popisuje účinek každé kombinace těchto parametrů:

DoDialog	DenySuspend	CheckChannels Spuštěno	Akce
N	N	N	Přijměte požadavek na pozastavení.
N	N	Y	Přijměte požadavek na pozastavení.
N	Y	N	Zamítněte požadavek na pozastavení.
N	Y	Y	Pokud jsou spuštěny nějaké kanály, zamítněte požadavek na pozastavení; pokud ne, přijměte požadavek.
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 dialogové okno (viz Poznámka ; přijmout požadavek).
Y	Y	N	Zobrazit dialogové okno (Poznámka ; odepřít požadavek na pozastavení).
Y	Y	Y	Pokud nejsou spuštěny žádné kanály, přijměte požadavek na pozastavení; pokud se zobrazí dialogové okno (Poznámka ; zamítnout požadavek).

Poznámka: V případech, kdy se má zobrazit dialogové okno, pokud toto dialogové okno nelze zobrazit (například protože je vaše víko zápisníku zavřené), použije se volba DenySuspend k určení, zda je požadavek na pozastavení přijat nebo zamítnut.

Multi Konfigurační soubory správce front, qm.ini

Konfigurační soubor správce front `qm.ini`obsahuje informace týkající se konkrétního správce front. Atributy, které můžete použít k úpravě konfigurace jednotlivého správce front, přepíší veškerá nastavení pro produkt IBM MQ.

Pro každého správce front existuje jeden konfigurační soubor správce front. Soubor `qm.ini` je automaticky vytvořen při vytvoření správce front, ke kterému je přidružen.

Poznámka: Další informace o tom, jak a kdy upravit soubor `qm.ini` a kdy se projeví změny provedené v souboru, viz "Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms" na stránce 83.

V systémech IBM MQ 9.0.4 a IBM MQ 9.0.0 Fix Pack 2kontroluje příkaz **strmqm** syntaxi sekcí CHANNELS a SSL v souboru `qm.ini` před úplným spuštěním správce front, což usnadňuje zjištění, co je špatné, a rychle ji opravte, pokud produkt **strmqm** zjistí, že soubor `qm.ini` obsahuje chyby. Další informace viz strmqm.

Umístění souborů `qm.ini`

Linux AIX V systémech AIX and Linux je soubor `qm.ini` uložen v kořenovém adresáři adresářového stromu obsazeného správcem front. Například cesta a název konfiguračního souboru pro správce front s názvem QMNAME je:

```
/var/mqm/qmgrs/QMNAME/qm.ini
```

Windows V systémech Windows je umístění souboru `qm.ini` určeno WorkPath určenou v klíči `HKLM\SOFTWARE\IBM\WebSphere MQ` . Například cesta a název konfiguračního souboru pro správce front s názvem QMNAME jsou následující:

```
C:\ProgramData\IBM\MQ\qmgrs\QMNAME\qm.ini
```

IBM i Soubor `qm.ini` je uložen v adresáři *mqmdata directory*`/`*QMNAME*`/qm.ini`, kde *mqmdata directory* je standardně `/QIBM/UserData/mqm` a *QMNAME* je název správce front, na kterého se inicializační soubor vztahuje.

Poznámka: Hodnotu *mqmdata directory* můžete změnit v souboru `mqs.ini` .

Název správce front může mít délku až 48 znaků. To však nezaručuje, že název je platný nebo jedinečný. Proto je vygenerován název adresáře na základě názvu správce front. Tento proces se nazývá *transformace názvu*. Popis viz IBM MQ názvy souborů a Názvy objektů v systému IBM i.

`qm.ini` sekcí

Upozornění:

- Toto téma odkazuje na další informace o oddílech v souboru `qm.ini` . Každá sekce obsahuje informace o parametrech v této sekci, případně včetně příkladu.
- Každá sekce zobrazuje platformu nebo platformy produktu IBM MQ for Multiplatforms , na které se tato sekce vztahuje.

Multi Automatická konfigurace souboru qm.ini při spuštění

V produktu IBM MQ 9.2.0můžete konfigurovat správce front tak, aby při každém spuštění správce front automaticky použil obsah souboru nebo sadu souborů obsahujících potlačení hodnoty `qm.ini` .

Pomocí této volby můžete nastavit konfiguraci, kterou lze upravit a automaticky přehrát při příštím spuštění správce front. Pokud jsou například přepisy `qm.ini` umístěny na připojené jednotce, je možné mít centralizovanou konfiguraci, kde je nejnovější verze použita na každého spuštěného správce front.

Tuto funkci můžete použít ke zjednodušení vytvoření jednotného klastru pomocí funkce automatického klastru. Příklad viz “Vytvoření nového uniformní klastru” na stránce 414.

Poznámka: Tyto přepisy jsou použity pouze při spuštění správce front a nemohou ovlivnit vytvoření správce front. Pomocí této funkce například nelze nastavit počet primárních souborů protokolu.

Než začnete

Můžete použít:

1. Jeden soubor a vytvořte textový soubor obsahující změny v souboru `qm.ini` .
2. Sada souborů ve formátu `qm.ini` :
   - Chcete-li identifikovat adresář, kde budou konfigurace existovat, a
   - V tomto adresáři vytvořte soubory, každý s příponou `.ini`, například `qminisettings.ini`.

Soubor nebo soubory musí obsahovat pouze nastavení sekcí a nastavení **attribute**=*value* pro položky, které se mění. Chcete-li například aktualizovat atribut **MaxChannels** v sekci Kanály, může soubor obsahovat:

```
Channels:
 MaxChannels=1234
```

Všimněte si, že v souborech pro přepis `qm.ini` se s libovolným řádkem, který má předponu `#` , zachází jako s komentářem.

Povolení automatické konfigurace atributů souboru qm.ini

Nového správce front můžete konfigurovat pomocí příznaku **-ii** příkazu **crtmqm** a ukazovat na konkrétní soubor nebo adresář. Dodaná hodnota je uložena v souboru `qm.ini` pod sekcí **AutoConfig** , jako atribut **IniConfig**.

Můžete nakonfigurovat existujícího správce front tak, aby umožňoval automatickou konfiguraci MQSC, a to přidáním **AutoConfig** atributu stanza **IniConfig**ukazujícího na platný soubor nebo adresář. Příklad:

```
AutoConfig:
   IniConfig=C:\MQ_Configuration\uniclus.ini
```

Jak funguje automatická konfigurace?

Během spuštění správce front je ověřena konfigurace, která je identifikována atributem sekce AutoConfig **IniConfig** , aby byla zajištěna platná syntaxe, a poté uložena ve stromu dat správce front do adresáře `autocfg` jako jeden soubor `cached.ini` .

Je-li zpracováno více souborů z adresáře, jsou zpracovány v abecedním pořadí.

Během prvního spuštění správce front brání neschopnost číst soubor nebo adresář ve spuštění správce front s příslušnou chybovou zprávou jak v konzole, tak v protokolu chyb správce front.

Je-li při následných restartech odkazovaný soubor nebo adresář nečitelný, použije se dříve uložený soubor v mezipaměti a zvýrazní se zpráva zapsaná do protokolu chyb správce front.

Při použití příkazu **strmqm** se obsah souboru `cached.ini` použije na soubor `qm.ini` jako přepis před vyvoláním správce front.

To znamená, že pro správce front v pohotovostním režimu jsou nastavení čtena při zpracování příkazu **strmqm** , nikoli při aktivaci správce front.

Jak se sestaví náhradní soubor qm.ini ?

Při první konfiguraci automatické inicializace a spuštění správce front je kopie aktuálního souboru `qm.ini` zkopírována do podadresáře `autoconfig` v datovém adresáři správce front jako `base_qm.ini`. Tato hodnota je od této chvíle považována za výchozí hodnotu.

Při každém spuštění správce front, tj. **strmqm** čas, je aktuálně aktivní soubor `qm.ini` vyřazen a nahrazen kopií souboru `base_qm.ini`. Pak se na tento soubor použije konfigurace ze souboru `cached.ini` .

Jakmile je správce front pod řízením automatické konfigurace, všechny změny v souboru `qm.ini` by měly být provedeny prostřednictvím souboru nebo souborů, které ukazují na použití atributu **IniConfig** v sekci AutoConfig .

Vzhledem k tomu, že existující soubor `qm.ini` je při spuštění správce front odebrán, bude pro základní řádek správce front použita pouze konfigurace v dodaném souboru `qm.ini` s použitím atributu **IniConfig** .

Pokud byla sekce nebo atribut změněn prostřednictvím konfigurace automatické inicializace při předchozích spuštěních správce front, tyto změny se odeberou, pokud nejsou stále identifikovány v souboru nebo souborech identifikovaných atributem **IniConfig** .

Kvůli opětnému vytvoření souboru `qm.ini` při spuštění správce front to znamená, že veškeré ruční změny souboru `qm.ini` budou ztraceny. Pokud skutečně potřebujete provést trvalou změnu a nemůžete použít atribut **IniConfig** k provedení této změny, můžete provést jednu z následujících akcí:

- Proveďte změnu v samotném souboru `base_qm.ini` .
- Odstraňte soubor `base_qm.ini` .

  Pokud tento soubor odstraníte, bude soubor `base_qm.ini` znovu vytvořen při příštím spuštění správce front na základě aktuálního obsahu souboru `qm.ini` . Toto *ztvrdne* všechny aktuální změny jako nová úroveň baseline pro budoucí spuštění.

Související pojmy

“Souhrn sekcí a atributů souboru qm.ini” na stránce 99
Souhrn atributů sekcí konfiguračního souboru správce front `qmi.ini`s odkazy na další informace.

Multi Souhrn sekcí a atributů souboru qm.ini

Souhrn atributů sekcí konfiguračního souboru správce front `qmi.ini`s odkazy na další informace.

Tabulka 11. Sekce souboru qm.ini

Sekce a atributy	Popis atributů
Windows **AccessMode sekce**	
Windows skupina přístupů [1]	Skupina zabezpečení Windows , jejímž členům bude udělen úplný přístup ke všem datovým souborům správce front.
ApiExitLokální sekce	
Název	Popisný název uživatelské procedury rozhraní API, která jí byla předána v poli ExitInfoNázev struktury MQAXP.
funkce	Název vstupního bodu funkce do modulu obsahujícího kód uživatelské procedury rozhraní API.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
Modul	Modul obsahující kód uživatelské procedury rozhraní API.
Data	Data, která mají být předána uživatelské proceduře rozhraní API v poli ExitData struktury MQAXP.
Posloupnost	Posloupnost, ve které je tato uživatelská procedura rozhraní API volána vzhledem k jiným uživatelským procedurám rozhraní API.
Linux V 9.3.4 AIX **AuthToken sekce**	
KeyStore	Cesta k souboru úložiště klíčů, které obsahuje certifikáty veřejného klíče důvěryhodného vydavatele nebo symetrické klíče.
KeyStorePwdFile	Cesta k souboru, který obsahuje šifrované heslo pro úložiště klíčů.
CertLabel	Popisek certifikátu pro certifikát veřejného klíče nebo symetrický klíč v úložišti klíčů, který se používá k ověření tokenů ověření.
UserClaim	Nárok v rámci tokenu, který obsahuje informace o identitě uživatele, které může správce front převzít pro kontroly autorizace.
AllowOSGroups	Tento atribut určuje, zda je členství ve skupině pro adoptovaného uživatele kontrolováno.
AutoCluster sekce	
Typ	Typ automatického klastru. Jedinou platnou volbou je volba Uniform, která představuje jednotný klastr.
ClusterName	Název automatického klastru.
RepositoryName1	Název správce front pro první úplné úložiště v automatickém klastru.
Repository1Conname	Hodnota názvu připojení (CONNAME) pro způsob připojení členů automatického klastru ke správci front.
RepositoryName2	Název správce front pro druhé úplné úložiště v automatickém klastru.
Repository2Conname	Hodnota názvu připojení (CONNAME) pro způsob připojení členů automatického klastru ke správci front.
AutoConfig sekce	
MQSCConfig	Buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.mqsc` použity na správce front při každém spuštění správce front.
IniConfig	Buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.ini` použity na soubor `qm.ini` při každém spuštění správce front.
Sekce kanálů	
MaxChannels	Maximální povolený počet aktuálních kanálů.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
MaxActiveChannels	Maximální počet kanálů, které mohou být kdykoli aktivní.
MaxInitiators	Maximální počet iniciátorů.
MQIBindType	Vazba pro aplikace.
PipeLineLength	Maximální počet souběžných podprocesů, které bude kanál používat.
AdoptNewMCA	Které typy kanálů mohou mít zastavenou existující instanci kanálu, aby se nová instance kanálu mohla spustit, když produkt IBM MQ obdrží požadavek na spuštění kanálu, ale zjistí, že instance kanálu je již spuštěna.
AdoptNewMCATimeout	Doba v sekundách, po kterou nová instance kanálu čeká na ukončení staré instance kanálu.
AdoptNewMCACheck	Při povolování atributu **AdoptNewMCA** je vyžadován typ kontroly.
ChlauthEarlyPřijmout	Pořadí, ve kterém jsou zpracována pravidla ověřování připojení a ověřování kanálu.
PasswordProtection	Zda musí být pověření určená aplikací chráněna ochranou pomocí hesla MQCSP, pokud kanál nepoužívá šifrování TLS.
IgnoreSeqNumberMismatch	Řídí způsob, jakým správce front zpracovává neshodu pořadových čísel při spuštění kanálu.
Sekce připojení	
DefaultBind	Určuje, zda aplikace a správce front, které jsou spouštěny v oddělených procesech, sdílejí některé prostředky nebo mezi nimi žádné prostředky.
DiagnosticMessages stanza	
name	Název stanzy.
Služba	Služba, která je povolena touto sekcí.
ExcludeMessage	Zprávy, které nemají být zapsány do protokolu chyb správce front.
SuppressMessage	Zprávy, které mají být zapsány do protokolu chyb správce front pouze jednou v určeném časovém intervalu.
IBM i SuppressInterval	Časový interval v sekundách, ve kterém jsou zprávy uvedené v souboru **SuppressMessage** zapisovány do protokolu chyb správce front pouze jednou.
Závažnosti	Seznam úrovní závažnosti oddělených čárkami.
FilePath	Cesta, kam se zapisují soubory protokolu. (Podpora je podporována pouze v případě, že je atribut Služba nastaven na hodnotu Soubor.)
FilePrefix	Předpona souborů protokolu. (Podpora je podporována pouze v případě, že je atribut Služba nastaven na hodnotu Soubor.)

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
FileSize	Velikost, při které se protokol přetočí. (Podpora je podporována pouze v případě, že je atribut Služba nastaven na hodnotu Soubor.)
Formát	Formát souboru. (Podpora je podporována pouze v případě, že je atribut Služba nastaven na hodnotu Soubor.)
Linux AIX Syslog	Služba syslog, která odesílá nefiltrované zprávy do protokolu syslog pomocí specifikace diagnostických zpráv formátu JSON .
Linux AIX Ident	Hodnota identifikátoru přidružená k položkám syslog. (podporováno pouze v případě, že je atribut Service nastaven na hodnotu Syslog.)
ExitPath stanza	
ExitsDefaultPath	Cesta pro uživatelské programy v systému správce front (32bitové).
ExitsDefaultPath64	Cesta pro uživatelské programy v systému správce front (64bitové).
ExitPropertiesLokální sekce	
CLWLMode	Zda uživatelská procedura CLWL (cluster workloac) běží buď v režimu FAST, nebo v režimu SAFE.
Linux IBM i AIX **Sekce systému souborů**	
Linux IBM i AIX ValidateAuth	Povolit uživatelům, kteří nejsou členy skupiny `mqm` , přístup k adresářům chyb a souborům.
Sekce protokolu	
LogPrimaryFiles	Soubory protokolu přidělené při vytvoření správce front.
LogSecondaryFiles	Soubory protokolu přidělené při vyčerpání primárních souborů.
LogFilePages	Počet stránek souboru protokolu. (Velikost souboru protokolu je určena v jednotkách stránek o velikosti 4 kB.)
LogType	Typ protokolování, které má použít správce front (kruhové nebo lineární).
LogBufferPages	Množství paměti přidělené záznamům vyrovnávací paměti pro zápis, určující velikost vyrovnávacích pamětí v jednotkách 4kB stránek.
LogPath	Adresář, ve kterém jsou umístěny soubory protokolu pro správce front.
LogWriteIntegrity	Metoda, kterou modul protokolování používá k spolehlivému zápisu záznamů protokolu.
LogManagement	Metoda používaná ke správě oblastí protokolu, a to buď ručně, nebo pomocí správce front.
Windows **LU62 sekce**	

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
Windows TPName	Název TP, který se má spustit na vzdáleném serveru.
Windows Library1	Název knihovny DLL APPC.
Windows Library2	Totéž jako Library1, používá-li se kód uložený ve dvou samostatných knihovnách.
CP4I **NativeHAInstance**	
“Název” na stránce 134	Název instance, který byl použit při vytvoření instance správce front.
“ReplicationAddress” na stránce 134	Název hostitele, IPv4 tečková desítková adresa nebo adresa instance v hexadecimálním formátu IPv6 .
CP4I **NativeHALocalSekce instance**	
“LocalName” na stránce 134	Název sekce instance NativeHALocalpřevzatý z názvu instance repliky protokolu uvedeného při vytvoření správce front nativní HA.
“KeyRepository” na stránce 135	Umístění úložiště klíčů, které obsahuje digitální certifikát, který se má použít pro ochranu provozu replikace protokolu.
“CertificateLabel” na stránce 135	Popisek certifikátu identifikující digitální certifikát, který se má použít pro ochranu provozu replikace protokolu.
“CipherSpec” na stránce 135	MQ CipherSpec , která má být použita k ochraně provozu replikace protokolu.
“LocalAddress” na stránce 135	Adresa lokálního síťového rozhraní, která přijímá provoz replikace protokolu.
“HeartbeatInterval” na stránce 135	Interval prezenčního signálu definuje, jak často, v milisekundách, aktivní instance správce front nativní vysoké dostupnosti odešle synchronizaci sítě.
“HeartbeatTimeout” na stránce 135	Časový limit prezenčního signálu definuje, jak dlouho bude instance repliky správce front nativní vysoké dostupnosti čekat, než se rozhodne, že aktivní instance nereaguje.
“RetryInterval” na stránce 136	Interval opakování definuje, jak často by se měl správce front nativní vysoké dostupnosti, v milisekundách, opakovat nezdařený odkaz na replikaci.
Windows **Sekce NETBIOS**	
Windows LocalName	Název, pod kterým je tento počítač známý v síti LAN.
Windows AdapterNum	Číslo adaptéru LAN.
Windows NumSess	Počet relací, které se mají přidělit.
Windows NumCmds	Počet příkazů, které se mají přidělit.
Windows NumNames	Počet názvů, které se mají přidělit.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
Windows Library1	Název knihovny DLL NetBIOS .
QMErrorLog	
ErrorLog	Určuje velikost protokolu chyb správce front, který je zkopírován do zálohy.
ExcludeMessage	Určuje zprávy, které nemají být zapsány do protokolu chyb správce front.
SuppressMessage	Určuje zprávy, které jsou zapsány do protokolu chyb správce front pouze jednou v určeném časovém intervalu.
SuppressInterval	Určuje časový interval v sekundách, v němž jsou zprávy určené v poli SuppressMessage zapisovány do protokolu chyb správce front pouze jednou.
Linux AIX **Sekce režimu omezení** [2]	
Linux AIX ApplicationGroup	Název lokální přenosové fronty, do které jsou vkládány vzdálené zprávy, není-li přenosová fronta explicitně definována pro své místo určení.
Sekce zabezpečení	
ClusterQueueAccessControl	Zkontrolujte řízení přístupu front klastru nebo úplných front hostovaných ve správcích front klastru.
Windows GroupModel	Zda OAM (Object Authority Manager) kontroluje globální skupiny při určování členství uživatele ve skupině na systému Windows.
Sekce služby	
Název	Název požadované služby.
EntryPoints	Počet vstupních bodů definovaných pro službu.
Windows SecurityPolicy	V systému Windowsse jedná o zásadu zabezpečení pro každého správce front.
Linux AIX SecurityPolicy	V systému AIX and Linux, zda správce front používá autorizaci založenou na uživateli nebo na skupině. V 9.3.0 V produktu IBM MQ 9.3.0můžete také vytvořit jméno uživatele jiného než operačního systému.
SharedBindingsUserId	Pouze pro sdílené vazby, zda je pole UserIdentifier ve struktuře IdentityContext z funkce MQZ_AUTHENTICATE_USER platné ID uživatele nebo skutečné ID uživatele.
FastpathBindingsUserId	Pouze pro vazby rychlé cesty, zda je pole UserIdentifier ve struktuře IdentityContext z funkce MQZ_AUTHENTICATE_USER platné ID uživatele nebo skutečné ID uživatele.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
IsolatedBindingsUserId	Pouze v případě izolovaných vazeb, bez ohledu na to, zda je pole UserIdentifier ve struktuře IdentityContext z funkce MQZ_AUTHENTICATE_USER efektivní ID uživatele nebo skutečné ID uživatele.
ServiceComponent	
Služba	Název požadované služby.
Název	Popisný název komponenty služby.
Modul	Název modulu, který má obsahovat kód pro tuto komponentu.
ComponentDataVelikost	Velikost datové oblasti komponenty předané komponentě při každém volání v bajtech.
Windows **Sekce SPX**	
Windows Soket	Číslo soketu SPX v hexadecimální notaci.
Windows BoardNum	Číslo adaptéru LAN.
Windows KeepAlive	Zapněte nebo vypněte funkci KeepAlive .
Windows Library1	Název knihovny DLL SPX.
Windows Library2	Stejné jako LibraryName1, používá se, pokud je kód uložen ve dvou samostatných knihovnách.
Windows ListenerBacklog	Přepsat výchozí počet nevyřízených požadavků pro modul listener SPX.
Sekce SSL	
V 9.3.0 OutboundSNI	Uvádí, zda klienti s podporou SNI nastaví SNI na název cílového kanálu IBM MQ pro vzdálený systém při zahájení připojení TLS nebo na název hostitele.
AllowOutboundSNI	Uvádí, zda klienti s podporou SNI nastaví SNI na název cílového kanálu IBM MQ pro vzdálený systém při inicializaci připojení TLS. **Upozornění:** Deprecated V 9.3.0 Od IBM MQ 9.3.0 je tato vlastnost zamítnuta. Místo toho použijte **OutboundSNI** .
AllowedCipherSpecifikace	Určuje vlastní seznam CipherSpecs , které jsou seřazeny a povoleny pro použití s kanály IBM MQ na platformě Multiplatforms.
AllowTLSV13	Zda může správce front používat specifikace TLS 1.3 CipherSpecs.
CDPCheckExtensions	Zda se kanály TLS v tomto správci front pokoušejí zkontrolovat servery CDP, které jsou pojmenovány v rozšířeních certifikátu CrlDistributionPoint.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
MinimumRSAKeyVelikost	Uvádí minimální velikost klíče, kterou musí mít certifikáty RSA, aby mohly být přijaty.
OCSPAuthentication	Akce, která se má provést, když nelze zjistit stav odvolání ze serveru OCSP.
OCSPCheckExtensions	Zda se kanály TLS v tomto správci front pokoušejí zkontrolovat servery OCSP, které jsou pojmenovány v rozšířeních certifikátu AuthorityInfoAccess.
OCSPTimeout	Počet sekund čekání na odpovídací modul OCSP při provádění kontroly odvolání.
ALW PeerCertChainValidation	Nastavení ověření platnosti certifikátu IBM Global Security Kit (GSKit) .
SSLHTTPProxyName	Buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má produkt GSKit použít pro kontroly OCSP.
SSLHTTPConnectTimeout	Počet sekund čekání na úspěšné vytvoření síťového připojení k serveru HTTP při provádění kontroly odvolání.
Sekce dílčího fondu “3” na stránce 108	Tuto sekci vytváří IBM MQ. Neměňte ji.
ShortSubpoolNázev “3” na stránce 108	Název odpovídající adresáři a symbolickému odkazu vytvořenému v adresáři /var/mqm/sockets , který produkt IBM MQ používá pro interní komunikaci mezi běžícími procesy.
stanza TCP	
Port	Výchozí číslo portu v desítkové notaci pro relace TCP/IP.
Windows Library1	Název knihovny DLL soketů TCP/IP.
KeepAlive	Zapněte nebo vypněte funkci KeepAlive .
ListenerBacklog	Přepsat výchozí počet neprovedených požadavků pro modul listener TCP/IP.
Časový limit připojení	Počet sekund do vypršení časového limitu pokusu o připojení soketu.
SndBuff	Velikost vyrovnávací paměti pro odesílání TCP/IP použité odesílajícím koncem kanálů v bajtech.
RcvBuffVelikost	Velikost vyrovnávací paměti pro příjem TCP/IP použité přijímacím koncem kanálů v bajtech.
RcvSndBuffSize	Velikost vyrovnávací paměti pro odesílání protokolu TCP/IP používané koncem odesilatele přijímacího kanálu v bajtech.
RcvRcvBuffSize	Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech, kterou používá přijímající strana přijímacího kanálu.
SvrSndBuffSize	Velikost vyrovnávací paměti pro odesílání TCP/IP v bajtech, kterou používá server na konci kanálu připojení serveru připojení klienta.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
SvrRcvBuffSize	Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech, kterou používá konec serveru kanálu připojení serveru připojení klienta.
Multi V 9.3.0 SecureCommsPouze	Uvádí, zda je povolena komunikace v prostém textu, výchozí hodnota, nebo není povolena.
Sekce parametrů ladění	
SuppressDspAuthFail	Zda správce front potlačí generování událostí autorizace a zápis chybových zpráv AMQ8077 do protokolu chyb při selhání kontroly autorizace, pokud připojení nemá k objektu oprávnění + dsp.
ImplSyncOpenOutput	Minimální počet aplikací, které mají otevřenou frontu pro vložení, než může být povolen implicitní synchronizační bod pro trvalé vložení mimo synchronizační bod.
UniformClusterNázev	Název klastru IBM MQ , který používáte jako uniformní klastr.
OAMLdapConnectČasový limit	Maximální doba v sekundách, po kterou bude klient LDAP čekat na vytvoření připojení TCP k serveru.
OAMLdapQueryTimeLimit	Maximální doba v sekundách, po kterou bude klient LDAP čekat na přijetí odpovědi na požadavek LDAP ze serveru.
V 9.3.2 OAMLdapResponseWarningTime	Pokud připojení k serveru LDAP trvalo déle, než je prahová hodnota v sekundách určená parametrem **OAMLdapResponseWarningTime** , bude do protokolu chyb zapsána zpráva AMQ5544W .
ExpiryInterval	Označuje frekvenci, s jakou správce front prochází fronty a hledá zprávy s vypršenou platností, které dosud nebyly vyčištěny jinými aktivitami fronty. Jedná se o časový interval v sekundách.
LivenessHeartBeatLen	Konfiguruje četnost provádění kontrol správce front, který zapisuje do protokolu, v rozumné míře.
ECHeartBeatLen	Konfiguruje frekvenci obecných kontrol stavu správce front.
FileLockHeartBeatLen	Změní výchozí hodnotu pro kontrolu zámků souborů pro správce front s více instancemi, kterou řadič provedení pravidelně provádí, aby se ujistil, že stále drží výlučný zámek na primárním souboru s více instancemi.
Sekce proměnných	
atribut=hodnota	Název a přidružená hodnota pro použití jako vložení během definic MQSC.
XAResourceManager stanza	
Název	Instance správce prostředků.
SwitchFile	Úplný název zaváděcího souboru obsahujícího strukturu přepínače XA správce prostředků.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
XAOpenString	Řetězec dat, která mají být předána do vstupního bodu xa_open správce prostředků.
XACloseString	Řetězec dat, která mají být předána do vstupního bodu xa_close správce prostředků.
ThreadOfControl	Hodnota, kterou správce front používá pro serializaci, když potřebuje volat správce prostředků z jednoho ze svých vlastních procesů s podporou podprocesů. Povinné pro Windows.

Notes:

1. Sekce AccessMode je nastavena volbou **-a [r]** v příkazu **crtmqm** . Po vytvoření správce front neměňte sekci AccessMode .
2. Sekce RestrictedMode je nastavena volbou **-g** v příkazu **crtmqm** . Po vytvoření správce front tuto sekci neměňte. Pokud nepoužijete volbu **-g** , sekce se nevytvoří v souboru `qm.ini` .
3. Sekce Subpool a atribut ShortSubpoolName v rámci této sekce jsou automaticky napsány produktem IBM MQ při vytváření správce front. IBM MQ zvolí hodnotu pro název ShortSubpool. Tuto hodnotu neměňte.

Windows Sekce AccessMode souboru qm.ini

Režim přístupu se vztahuje pouze na servery Windows . Sekce AccessMode souboru qm.ini je nastavena volbou `-a [ r]` v příkazu **crtmqm** . Po vytvoření správce front neměňte sekci AccessMode .

Použít skupinu přístupů (`-a [ r]`) Volba příkazu **crtmqm** pro určení skupiny zabezpečení Windows , jejíž členům bude udělen úplný přístup ke všem datovým souborům správce front. Skupina může být buď lokální, nebo globální, v závislosti na použité syntaxi. Platná syntaxe pro název skupiny je následující:

LocalGroup
Název domény\GlobalGroup název
GlobalGroup název @ Název domény

Před spuštěním příkazu **crtmqm** s volbou `-a [ r]` musíte definovat další skupinu přístupů.

Zadáte-li skupinu pomocí volby `-ar` namísto volby `-a`, nebude lokální skupině mqm 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, bude ID uživatele kontrolované systémem Windows ID uživatele, kterého jste nakonfigurovali v průvodci **Příprava produktu** IBM MQ. Pokud jste spustili správce front interaktivně, bude ID uživatele kontrolované systémem Windows ID uživatele, který spustil příkaz **strmqm**.

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.

Příklad stanza

```
AccessMode:
SecurityGroup=wmq\wmq
```

Související pojmy

“Zabezpečte nesdílená data a adresáře a soubory protokolů správce front v systému Windows” na stránce 526

“Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows” na stránce 523

Související úlohy

“Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498

Související odkazy

crtmqm (vytvořit správce front)

Multi ApiExitLokální sekce souboru qm.ini

Lokální sekce ApiExiturčuje uživatelské procedury rozhraní API pro správce front.

V případě serveru upravte lokální sekci ApiExitsouboru `qm.ini` tak, aby identifikovala uživatelské procedury rozhraní API pro správce front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer `Exits` .

V případě klienta upravte lokální sekci ApiExitv souboru `mqclient.ini` tak, aby identifikovala uživatelské procedury rozhraní API pro správce front.

Přehled

Sekce `ApiExitLocal` umožňuje zadat pouze jednu položku `Module` , a přesto je třeba poskytnout čtyři moduly, a to následujícím způsobem:

- 32 bitů bez podprocesů
- 32 bitový podproces
- 64bitový bez podprocesů
- 64bitový podproces

Všimněte si, že IBM MQ připojí `_r` k dodanému názvu modulu, aby identifikoval verzi uživatelské procedury s podporou podprocesů, ale produkt IBM MQ neposkytuje přímo ekvivalentní mechanizmus pro 32bitové a 64bitové varianty.

Verze produktů `amqsaxe0` a `amqsaxe0_r` , které jsou dodávány v produktu *prefix*`/mqm/samp/bin` , jsou sestaveny pro nativní velikost správce front na platformě, pro kterou jsou sestaveny (nyní všechny 64bitové), a mohou je používat pouze aplikace spuštěné ve stejné nativní velikosti.

Je-li uveden nekvalifikovaný název modulu, IBM MQ hledá v souboru `/var/mqm/exits` 32bitové varianty a v souboru `/var/mqm/exits64` 64bitové varianty.

Například `module=amqsaxe` znamená:

```
/var/mqm/exits/amqsaxe  - 32 bit unthreaded variant
/var/mqm/exits/amqsaxe_r - 32 bit threaded variant
/var/mqm/exits64/amqsaxe - 64 bit unthreaded variant
/var/mqm/exits64/amqsaxe_r - 64 bit threaded variant
```

Windows V systémech Windows můžete také pomocí příkazu **amqmdain** změnit položky pro uživatelské procedury rozhraní API. (Chcete-li identifikovat uživatelské procedury rozhraní API pro všechny správce front, použijte sekce ApiExitCommon a ApiExitTemplate, jak je popsáno v tématu “ApiExitCommon a ApiExitstanzas šablony souboru mqs.ini” na stránce 91.)

Všimněte si, že aby uživatelská procedura rozhraní API správně fungovala, musí být zpráva ze serveru odeslána klientovi bez převodu. Po zpracování zprávy uživatelskou procedurou rozhraní API musí být zpráva převedena na klienta. To proto vyžaduje, abyste nainstalovali všechny uživatelské procedury převodu na klienta.

Další informace o použití těchto atributů naleznete v tématu Konfigurace uživatelských procedur rozhraní API.

Parametry

Název = ApiExit_name
Popisný název uživatelské procedury rozhraní API, která jí byla předána v poli ExitInfoNázev struktury MQAXP.

Tento název musí být jedinečný, nesmí být delší než 48 znaků a musí obsahovat pouze platné znaky pro názvy objektů IBM MQ (například názvy front).

Funkce=název_funkce
Název vstupního bodu funkce do modulu obsahujícího kód uživatelské procedury rozhraní API. Tento vstupní bod je funkcí MQ_INIT_EXIT.

Délka pole je omezena hodnotou MQ_EXIT_NAME_LENGTH.

Module=název_modulu
Modul obsahující kód uživatelské procedury rozhraní API.

Pokud pole obsahuje název modulu včetně úplné cesty, je použit beze změny. Pokud toto pole obsahuje pouze název modulu, je modul umístěn pomocí atributu **ExitsDefaultPath** v sekci `ExitPath` souboru `qm.ini` .

Na platformách, které podporují samostatné knihovny s podporou podprocesů, musíte poskytnout verzi modulu uživatelské procedury rozhraní API bez podpory podprocesů i s podporou podprocesů. Verze s podprocesy musí mít příponu `_r` . Verze se podprocesy stubu aplikace IBM MQ implicitně připojí `_r` k danému názvu modulu před jeho načtením.

Délka tohoto pole je omezena na maximální délku cesty, kterou platforma podporuje.

Data=název_dat
Data, která mají být předána uživatelské proceduře rozhraní API v poli ExitData struktury MQAXP.

Pokud zahrnete tento atribut, počáteční a koncové mezery se odeberou, zbývající řetězec se ořízne na 32 znaků a výsledek se předá uživatelské proceduře. Vynecháte-li tento atribut, přednastavená hodnota 32 mezer se předá uživatelské proceduře.

Maximální délka tohoto pole je 32 znaků.

Sekvence=pořadové_číslo
Posloupnost, ve které je tato uživatelská procedura rozhraní API volána vzhledem k jiným uživatelským procedurám rozhraní API. Ukončení s nízkým pořadovým číslem je voláno před ukončením s vyšším pořadovým číslem. Není třeba, aby pořadové číslování východů bylo souvislé. Posloupnost 1, 2, 3 má stejný výsledek jako posloupnost 7, 42, 1096. Pokud mají dvě uživatelské procedury stejné pořadové číslo, rozhodne se správce front, která z nich má být volala jako první. Můžete určit, který byl volán po události, vložením času nebo značkovače do oblasti ExitChainoznačené ExitChainAreaPtr v MQAXP nebo zápisem vlastního souboru protokolu.

Tento atribut je číselná hodnota bez znaménka.

Příklad stanza

```
ApiExitLocal:
   Name=ClientApplicationAPIchecker
   Sequence=3
   Function=EntryPoint
   Module=/usr/Dev/ClientAppChecker
   Data=9.20.176.20
```

Linux V 9.3.4 AIX Sekce AuthToken souboru qm.ini

Pomocí sekce **AuthToken** konfigurujte správce front tak, aby ověřoval tokeny ověřování poskytované připojováním aplikací.

Sekce AuthToken

KeyStore= řetězec

Cesta k souboru úložiště klíčů, které obsahuje certifikáty veřejného klíče důvěryhodného vydavatele a symetrické klíče. Klíče můžete přidat do existujícího úložiště klíčů nebo vytvořit nové úložiště klíčů. Další informace naleznete v tématu Konfigurace správce front pro přijímání tokenů ověřování. Správce front používá klíče v úložišti klíčů k ověření, že token ověření, který aplikace představuje, je podepsán důvěryhodným vydavatelem.

Můžete použít buď úložiště klíčů CMS s příponou souboru `.kdb` , nebo úložiště klíčů PKCS#12 s příponou souboru `.p12`. Pokud soubor úložiště klíčů neexistuje nebo k němu nelze přistupovat, je do protokolu chyb správce front generována chyba `AMQ7076E: Neplatná hodnota atributu v souboru ini.`

Ujistěte se, že se typ úložiště klíčů shoduje s příponou názvu souboru pro úložiště klíčů. Produkt IBM MQ zjistí správný formát úložiště klíčů, nekonzistence však mohou způsobit další administrativní problémy, pokud se typ úložiště klíčů a přípona názvu souboru neshodují.

Maximální délka cesty k souboru úložiště klíčů je 256 znaků.

KeyStorePwdFile= řetězec

Cesta k souboru, který obsahuje šifrované heslo pro úložiště klíčů. Soubor musí obsahovat šifrované heslo jako jeden řádek textu. Hesla v prostém textu nejsou přijata.

Použijte příkaz **runqmcred** k zašifrování hesla před jeho uložením do souboru hesel úložiště klíčů. Soubor hesel úložiště klíčů musí obsahovat pouze zašifrované heslo, které je vytvořeno spuštěním příkazu **runqmcred** .

Maximální délka hesla v prostém textu před šifrováním je 1024 znaků.

Tento parametr je volitelný. Není-li uveden, správce front vyhledá soubor pro dočasné ukládání s heslem ve stejném adresáři a se stejným názvem jako úložiště klíčů, ale s příponou souboru `.sth`. Není-li soubor pro dočasné ukládání nalezen, konfigurace je odmítnuta a do protokolu chyb správce front se zobrazí chybová zpráva AMQ7006E . Další informace o volbách ukládání hesel úložiště klíčů naleznete v tématu Šifrování hesel úložiště klíčů.

Maximální délka cesty k souboru hesel je 256 znaků.

CertLabel= řetězec

Popisek certifikátu pro certifikát veřejného klíče nebo symetrický klíč v úložišti klíčů, který se používá k ověření tokenů ověření. Opakováním atributu **CertLabel** můžete poskytnout až 32 popisků certifikátů.

Při přidávání certifikátů do úložiště klíčů správce front jim zadejte smysluplné popisky. Popisky certifikátů rozlišují malá a velká písmena. Mohou obsahovat alfanumerické znaky, interpunkční znaky a mezery. Pokud je zjištěn neplatný znak, vrátí se chyba a do protokolu chyb IBM MQ se zapíše chybová zpráva.

Vydavatelé důvěryhodných tokenů mohou poskytovat více certifikátů veřejných klíčů a symetrických klíčů. Například certifikáty veřejných klíčů mají období platnosti. Pokud se blíží vypršení platnosti, vydavatel tokenu poskytne nový certifikát s novým datem vypršení platnosti. Oba certifikáty mohou být po určitou dobu platné.

Když aplikace prezentují tokeny pro ověření, je seznam **CertLabels** zkontrolován, dokud není nalezen platný klíč, který byl použit k podepsání tokenu. Je-li nalezena shoda, podpis tokenu je ověřen.

Pokud není zadán parametr **CertLabel** , připojení z aplikace, která token prezentuje, se nezdaří s kódem příčiny 2063 MQRC_SECURITY_ERRORa do protokolu chyb správce front se zapíše zpráva AMQ5786E: Chyba konfigurace tokenu ověření.

Maximální délka popisku certifikátu je 64 znaků.

Například:

```
AuthToken:
   KeyStore=/var/mqm/qmgrs/qmgrs/qm1/tokenissuer/key.kdb
   KeyStorePwdFile=/var/mqm/qmgrs/qm1/tokenissuer/key.pw
   CertLabel=token
   CertLabel=rsakey
   CertLabel=mark
   ... up to 32 CertLabel fields
```

UserClaim= řetězec
Nárok v rámci tokenu, který obsahuje ID uživatele, které správce front převezme pro kontroly autorizace.

Tento parametr je volitelný, pokud je správce front konfigurován s parametrem **ADOPTCTX(NO)**. Je-li použit parametr **ADOPTCTX(YES)** , je tento parametr povinný. **ADOPTCTX** je atribut přítomný v objektu ověřovacích informací (AUTHINFO), na který odkazuje atribut **CONNAUTH** správce front.

Chcete-li převzít identitu, token musí obsahovat nárok s názvem, který je uveden v atributu **UserClaim** sekce **AuthToken** a **ADOPTCTX(YES)** .

Pokud například váš token obsahuje nárok "AppUser": "MyUserName", musíte zadat UserClaim=AppUser v sekci AuthToken souboru qm.ini , abyste převzali identitu "MyUserName" pro autorizaci.

Maximální délka hodnoty atributu **UserClaim** je 128 znaků.

Poznámka: Pokud je v produktu IBM MQ 9.3.4uvedena sekce AuthToken , efektivní hodnota atributu **SecurityPolicy** sekce Service je nastavena na UserExternal. Ověření tokenu není k dispozici, pokud je **SecurityPolicy** explicitně nastaveno na Skupina v sekci Služba. Je-li parametr **SecurityPolicy** nastaven na hodnotu Skupina, odeberte atribut **SecurityPolicy** ze sekce služby a poté restartujte správce front. Další informace viz SecurityPolicy.

Poznámka: Pomocí atributu **ADOPTCTX** objektu ověřovacích informací můžete řídit, zda je ID uživatele v tokenu převzat pro kontroly autorizace. Při vytváření správce front je tento atribut nastaven na hodnotu **ADOPTCTX(YES)**. Tato hodnota způsobí, že ID uživatele z tokenu bude převzat. ID uživatele musí splňovat požadavky na ID uživatelů v tokenech ověření. Další informace viz ID uživatelů v tokenech ověření. Pokud nárok uživatele tokenu obsahuje ID uživatele, které nesplňuje požadavky, bude připojení odmítnuto s kódem příčiny **2035 MQRC_NOT_AUTHORIZED**. Je-li nastavena hodnota **ADOPTCTX(NO)** , token se použije pouze pro ověření a pro autorizaci se musí použít jiný uživatel.

AllowOSGroups=NO (výchozí) |YES
Výchozí hodnota je NO. Určuje, zda je identita, která je převzata z tokenu, považována za uživatele operačního systému (OS) a zda je členství ve skupinách odpovídajícího uživatele operačního systému uznáno během autorizace.

AllowOSGroups= NO | N
Kontroly autorizace jsou založeny pouze na jménu uživatele, který je převzata z tokenu.

AllowOSGroups= YES | Y
Kontroly autorizace jsou založeny na jménu uživatele a kontrolují se také skupiny, do kterých mohou patřit.

Příklad stanza-pouze ověření

Vaše sekce **AuthToken** může být platná pouze se dvěma minimálními požadovanými parametry:

- Cesta k souboru **KeyStore** a
- **CertLabel** název.

```
AuthToken:
   KeyStore=/var/mqm/qmgrs/qmgrs/qm1/tokenissuer/key.kdb
   CertLabel=token
   ... up to 32 CertLabel fields
```

Pokud jste zahrnuli pouze dva minimální parametry, pak:

- Soubor pro dočasné ukládání `key.sth` musí existovat se zašifrovaným heslem úložiště klíčů, aby nebyl soubor s heslem úložiště klíčů povinný.
- Token neobsahuje jméno uživatele, které má být předáno produktu IBM MQ k autorizaci. Aplikace se může připojit a být ověřena, ale musí být k dispozici jiný mechanizmus, který poskytne aplikaci autorizaci k provedení práce po připojení.

V závislosti na konfiguraci vašeho správce front může být jméno uživatele, které se používá pro autorizaci, jméno uživatele definované v kanálu prostřednictvím pravidel MCA nebo jméno uživatele, které aplikace klienta spustila na vašem serveru a patří do skupin s oprávněními. Mějte na paměti, že při použití tokenů:

- Váš správce front je převeden do režimu **UserExternal** , což znamená, že pro ověření lze použít uživatele, kteří neexistují v operačním systému, v němž je spuštěn správce front.
- I když nezahrnete volbu **AllowOSGroups** do sekce **AuthToken** `qm.ini` , předvolba je nastavena na Ne. Pokud tedy zahrnete **UserClaim** , ale neuvedete **AllowOSGroups**=Ano, uživatel tokenu, který je adoptován pro autorizaci, nebude kontrolován pro skupiny, do kterých by mohl náležet v operačním systému, kde je spuštěn správce front.

Příklad stanza-ověření a autorizace

Můžete definovat všechny parametry **AuthToken** :

- cesta k souboru **KeyStore** ,
- cesta k souboru **KeyStorePwdFile** ,
- **CertLabel** název,
- **UserClaim** název a
- Volba **AllowOSGroups** .

```
AuthToken:
   KeyStore=/var/mqm/qmgrs/qmgrs/QMJWT/ssl/key.kdb
   KeyStorePwdFile=/var/mqm/qmgrs/QMJWT/ssl/key.pw
   CertLabel=token
   CertLabel=rsakey
   CertLabel=mark
   ... up to 32 CertLabel fields
   UserClaim=AppUser
   AllowOSGroups=Y
```

Pokud jste zahrnuli všechny dostupné parametry, pak:

- Zašifrujte heslo úložiště klíčů pomocí příkazu **runqmcred** . Uložte jej do souboru, pak zahrňte cestu k souboru do sekce **AuthToken** .
- Jméno uživatele, které je v nároku uživatele tokenu ověření, se používá jak pro ověření, tak pro autorizaci.
  - Uživatel tokenu může existovat jako uživatel v operačním systému, kde je spuštěn správce front.
  - Definovali jste objekt ověřovacích informací pro povolení kontroly uživatele.
  - Záznamy ověřování kanálu nastavíte tak, aby adoptovaly uživatele s oprávněním k interakci s objekty produktu IBM MQ na základě pravidel ověřování kanálu nebo MCA.

Vaše strategie ověřování a autorizace uživatelů tokenů závisí na vašich požadavcích a na tom, jak jsou správci front produktu IBM MQ již nakonfigurováni. Další informace viz Práce s tokeny ověření.

Související pojmy

Práce s tokeny

Související úlohy

Konfigurace správce front pro přijetí **AuthTokens**

Použití tokenů ověření v aplikaci

Multi Sekce AutoCluster souboru qm.ini

Sekce AutoCluster se používá, když správce front začne zjišťovat, zda je klastr členem automatického klastru, a může identifikovat úplná úložiště klastru.

Následující atributy jsou povinné pro sekci AutoCluster :

Typ =*Jednotná*
: Určuje typ automatického klastru a jedinou platnou volbou je volba *Jednotný*, která představuje uniformní klastr.

ClusterName=*< Řetězec >*
: Název klastru, což je automatický název klastru.

Následující atributy jsou volitelné pro sekci AutoCluster , ale musíte je poskytnout ve dvojicích:

NázevRepository1 =*< řetězce>*
: Jedná se o název správce front pro první úplné úložiště v automatickém klastru. Může se jednat o název tohoto správce front nebo jiného správce front.

Repository1Conname=*< Řetězec názvu připojení >*
: Jedná se o hodnotu názvu připojení (CONNAME) pro způsob připojení členů automatického klastru k tomuto správci front.

Název_úložného_úložiště=*< řetězce>*
: Jedná se o název správce front pro druhé úplné úložiště v automatickém klastru. Může se jednat o název tohoto správce front nebo jiného správce front.

Repository2Conname=*< Řetězec názvu připojení >*
: Jedná se o hodnotu názvu připojení (CONNAME) pro způsob připojení členů automatického klastru k tomuto správci front.

Příklad stanza

```
AutoCluster:
        Repository1Name=QM1
        Repository2Name=QM2
        Repository1Conname=127.0.0.1(1414)
        Repository2Conname=127.0.0.1(1415)
        ClusterName=UNIFORMCLUSTER1
        Type=Uniform
```

Související pojmy

“Automatické vyvažování aplikací” na stránce 402

Automatické vyvažování aplikací výrazně rozšiřuje distribuci a dostupnost aplikací tím, že umožňuje jednotnému klastru IBM MQ pečlivě spravovat distribuci aplikací v rámci klastru a nespoléhat se na randomizaci ani na ruční připnutí aplikací ke specifickým správcům front.

Související úlohy

“Vytvoření nového uniformní klastru” na stránce 414

Jak vytvoříte nový jednotný klastr.

Související odkazy

“Použití automatické konfigurace klastru” na stránce 418

Produkt IBM MQ nakonfigurujete tak, aby umožňoval automatickou konfiguraci změnou informací o konfiguraci `qm.ini` .

Multi Sekce AutoConfig souboru qm.ini

Atributy sekce AutoConfig se často používají jako součást nastavení uniformních klastrů.

Poznámka: Sekci AutoCluster můžete použít pouze pro uniformní klastry.

MQSCConfig=*< Cesta_ >*
Cesta je buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.mqsc` použity na správce front při každém spuštění správce front.

Další informace naleznete v tématu Automatická konfigurace ze skriptu MQSC při spuštění.

IniConfig=*< cesta_k>*
Cesta je buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.ini` použity na soubor `qm.ini` při každém spuštění správce front.

Další informace viz téma “Automatická konfigurace souboru qm.ini při spuštění” na stránce 98.

V 9.3.0 **ConfigTimeout**
Hodnota (v sekundách), po kterou správce front čeká na dokončení automatické konfigurace. Po uplynutí této doby bude správce front pokračovat ve spouštění a bude k dispozici pro připojení aplikací.

Výchozí chování je bez časového limitu. To znamená, že správce front není k dispozici pro připojení aplikací, dokud nebudou dokončeny všechny příkazy automatické konfigurace.

Tento atribut byste neměli konfigurovat jednoduše proto, že konfigurace trvá dlouho, protože aplikace se mohou být schopny připojit před dokončením konfigurace, která se na ně vztahuje, například vytvoření front potřebných pro aplikaci.

Příklad stanza

```
AutoConfig:
        MQSCConfig=/tmp/auto.mqsc
        IniConfig=/tmp/auto.ini
        ConfigTimeout=120
```

Související pojmy
“Automatické vyvažování aplikací” na stránce 402
Automatické vyvažování aplikací výrazně rozšiřuje distribuci a dostupnost aplikací tím, že umožňuje jednotnému klastru IBM MQ pečlivě spravovat distribuci aplikací v rámci klastru a nespoléhat se na randomizaci ani na ruční připnutí aplikací ke specifickým správcům front.

Související úlohy
“Vytvoření nového uniformní klastru” na stránce 414
Jak vytvoříte nový jednotný klastr.

Související odkazy
“Použití automatické konfigurace klastru” na stránce 418
Produkt IBM MQ nakonfigurujete tak, aby umožňoval automatickou konfiguraci změnou informací o konfiguraci `qm.ini` .

Multi Sekce kanálů souboru qm.ini

Atributy sekce Kanály určují konfiguraci kanálu.

z/OS Tyto informace nelze použít pro IBM MQ for z/OS.

Sekci `CHANNELS` v souboru `qm.ini` použijte k uvedení informací o kanálech.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer `Channels` .

MaxChannels = 100 (výchozí) |*číslo*
Maximální povolený počet *aktuálních* kanálů.

Výchozí hodnota je 100.

Můžete nastavit **MaxChannels** na jinou hodnotu, chcete-li v případě potřeby omezit maximální počet aktuálních kanálů. Pro systém IBM MQ Applianceje výchozí hodnota 999 999 999 a neměla by se měnit.

MaxActiveKanály = *MaxChannels_value*
Maximální počet kanálů, které mohou být kdykoli *aktivní* . Výchozí hodnota je extrahována z atributu **MaxChannels**.

MaxInitiators = 3 (výchozí) |*číslo*
Maximální počet iniciátorů. Výchozí a současně maximální hodnota je 3.

MQIBindType= FASTPATH | STANDARD
Vazba pro aplikace:

Rychlý
Kanály se připojují pomocí příkazu `MQCONNX FASTPATH`; neexistuje žádný proces agenta.

STANDARD
Kanály se připojují pomocí STANDARD.

Délka řádku PipeLineLength = 1 |*číslo*
Maximální počet souběžných podprocesů, které bude kanál používat. Výchozí hodnota je 1. Jakákoli hodnota větší než 1 je považována za hodnotu 2.

Při použití propojení procesů konfigurujte správce front na obou koncích kanálu tak, aby měl hodnotu **PipeLineLength** větší než 1.

Poznámka: Propojení procesů je efektivní pouze pro kanály TCP/IP.

Další informace naleznete v tématu Podpora více podprocesů-propojení procesů .

AdoptNewMCA = NO (výchozí) | SVR | SDR | RCVR | CLUSRCVR | ALL | FASTPATH
Pokud produkt IBM MQ obdrží požadavek na spuštění kanálu, ale zjistí, že instance kanálu je již spuštěna, musí být v některých případech existující instance kanálu zastavena, než bude možné spustit novou instanci kanálu. Atribut **AdoptNewMCA** vám umožňuje řídit, které typy kanálů lze tímto způsobem ukončit.

Zadáte-li atribut **AdoptNewMCA** pro konkrétní typ kanálu, ale spuštění nového kanálu se nezdaří, protože odpovídající instance kanálu je již spuštěna:

1. Nový kanál se pokusí zastavit předchozí kanál tím, že jej požádá o ukončení.
2. Pokud předchozí kanálový server neodpoví na tento požadavek v době, kdy vyprší čekací interval **AdoptNewMCATimeout** , podproces nebo proces pro předchozí kanálový server se ukončí.
3. Pokud předchozí server kanálu neskončil po kroku 2 a po druhém vypršení intervalu čekání **AdoptNewMCATimeout** , ukončí produkt IBM MQ kanál s chybou `CHANNEL IN USE` .

Funkce **AdoptNewMCA** platí pro kanály server, odesilatel, příjemce a přijímací kanály klastru. V případě odesílacího kanálu nebo kanálu serveru může být v přijímajícím správci front spuštěna pouze jedna instance kanálu s konkrétním názvem. V případě přijímacího kanálu nebo přijímacího kanálu klastru může být v přijímajícím správci front spuštěno více instancí kanálu s konkrétním názvem, ale pouze jedna instance může být spuštěna současně z konkrétního vzdáleného správce front.

Poznámka: Produkt **AdoptNewMCA** není podporován v žadatelském kanálu nebo kanálu připojení serveru.

Uveďte jednu nebo více hodnot oddělených čárkami nebo mezerami z následujícího seznamu:

NO
Funkce `AdoptNewMCA` není požadována. Toto nastavení je výchozí.

SVR
Adoptovat kanály serveru.

SDR
Adoptovat odesílací kanály.

RCVR
Adoptovat přijímací kanály.

CLUSRCVR
Adoptovat přijímací kanály klastru.

ALL
Převezměte všechny typy kanálů kromě kanálů FASTPATH.

Rychlý
Převezměte kanál, pokud se jedná o kanál FASTPATH. K tomu dochází pouze v případě, že je zadán také příslušný typ kanálu, například: `AdoptNewMCA=RCVR,SVR,FASTPATH`.

Pozorujte mě!: Atribut AdoptNewMCA se může chovat nepředvídatelným způsobem s kanály FASTPATH. Při povolování atributu MCA AdoptNewpro kanály FASTPATH postupujte velmi opatrně.

AdoptNewMCATimeout= 60 (výchozí) | 1-3600
Doba v sekundách, po kterou nová instance kanálu čeká na ukončení staré instance kanálu. Zadejte hodnotu v rozsahu 1-3600. Výchozí hodnota je 60.

AdoptNewMCACheck = QM | ADDRESS | NAME | ALL
Při povolování atributu `AdoptNewMCA` je vyžadován typ kontroly. Pokud je to možné, proveďte úplnou kontrolu, abyste ochránili své kanály před vypnutím, neúmyslně nebo úmyslně. Alespoň zkontrolujte, zda se názvy kanálů shodují.

Zadejte jednu nebo více následujících hodnot oddělených čárkami nebo mezerami v případě *QM*, *NAME*nebo *ALL*:

Řízení kvality
Zkontrolujte, zda se názvy správců front shodují.

Všimněte si, že název správce front je shodný, nikoli s identifikátorem QMID.

ADDRESS
Zkontrolujte adresu IP zdroje komunikací. Například adresa TCP/IP.

Poznámka: Hodnoty CONNAME oddělené čárkami platí pro cílové adresy, a proto nejsou pro tuto volbu relevantní.

V případě, že dojde k selhání správce front s více instancemi z `hosta` na `hostb`, budou všechny odchozí kanály z tohoto správce front používat zdrojovou adresu IP `hostb`. Pokud se liší od `hosta`, pak se AdoptNewMCACheck=*ADDRESS* neshoduje.

Můžete použít SSL nebo TLS se vzájemným ověřením, abyste zabránili útočníkovi v narušení existujícího spuštěného kanálu. Alternativně použijte řešení typu HACMP s převzetím IP namísto správců front s více instancemi, nebo použijte prostředek pro vyrovnávání zátěže sítě k maskování zdrojové adresy IP.

NÁZEV
Zkontrolujte, zda se názvy kanálů shodují.

ALL
Zkontrolujte odpovídající názvy správců front, komunikační adresu a odpovídající názvy kanálů.

Výchozí hodnota je `AdoptNewMCACheck=NAME,ADDRESS,QM`.

ChlauthEarlyAdopt = Y (výchozí) | N
Pořadí, ve kterém jsou pravidla ověřování připojení a ověřování kanálu zpracována, je významným faktorem při určování kontextu zabezpečení pro připojení klientských aplikací IBM MQ .

Upozornění: Výchozí hodnota, pokud soubor qm.ini neobsahuje hodnotu **`ChlauthEarlyAdopt`** , je `N`, avšak z IBM MQ 9.0.4 všech správců front se vytvoří automaticky s hodnotou **`ChlauthEarlyAdopt`**=Y , která se přidá do souboru qm.ini .

Produkt **ChlauthEarlyAdopt** pouze převezme ID uživatelů, která byla poskytnuta správci front pro ověření připojení, pokud je pro objekt AUTHINFO ověřování připojení ve správci front nastaveno hodnota YES (sadaCTX).

Platné hodnoty pro **ChlauthEarlyAdopt** jsou následující hodnoty:

Y
Kanál před použitím pravidel ověřování kanálu ověří a převezme pověření ID uživatele a hesla, která byla poskytnuta aplikací s použitím ověřování připojení správce front. V tomto režimu operace se pravidla ověřování kanálu shodují s ID uživatele, které je výsledkem kontrol ověřování připojení.

N
Kanál zpožďuje ověřování připojení pro pověření ID uživatele a hesla, která byla poskytnuta aplikací, až do doby, kdy byla použita pravidla ověřování kanálu. Všimněte si, že v tomto režimu operace nemohou blokování ověřování kanálu a pravidla mapování brát v úvahu výsledky ověření ID uživatele a hesla.

Výchozí objekt ověřovacích informací je například nastaven na hodnotu **ADOPTCTX(YES)** a uživatel `fred` je přihlášen. Jsou nakonfigurována následující dvě pravidla CHLAUTH:

```
SET CHLAUTH('MY.CHLAUTH') TYPE(ADDRESSMAP) DESCR('Block all access by
default') ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
SET CHLAUTH('MY.CHLAUTH') TYPE(USERMAP) DESCR('Allow user bob and force
CONNAUTH') CLNTUSER('bob') CHCKCLNT(REQUIRED) USERSRC(CHANNEL)
```

Je vydán následující příkaz s úmyslem ověřit příkaz jako přijatý kontext zabezpečení uživatele bob:

```
runmqsc -c -u bob QMGR
```

Správce front ve skutečnosti používá kontext zabezpečení `fred`, nikoli bob, a připojení se nezdaří.

Chcete-li použít kontext zabezpečení bob, **ChlauthEarlyAdopt** musí být nastaven na Y.

PasswordProtection = Kompatibilní (výchozí) |vždy|volitelné|varování

V produktu IBM MQ 8.0lze ověřovací pověření, která aplikace IBM MQ client zadávají při připojení ke správci front, chránit pomocí funkce ochrany heslem produktu IBM MQ MQCSP, pokud připojení nepoužívá šifrování TLS.

Ochrana heslem MQCSP je užitečná pro účely testování a vývoje, protože použití ochrany heslem MQCSP je jednodušší než nastavení šifrování TLS, ale ne tak bezpečné.

Další informace o ochraně pověření ve struktuře MQCSP a o hodnotách, které lze nastavit pro tento atribut, naleznete v tématu Ochrana heslem MQCSP.

IgnoreSeqNumberMismatch = NO (výchozí) | YES
Agenti MCA (Message Channel Agents) na obou koncích kanálu udržují počet zpráv odeslaných kanálem za účelem zachování synchronizace. Synchronizace může být ztracena, například pokud je definice kanálu na jednom konci odstraněna a poté znovu vytvořena. Za těchto okolností může být požadováno, aby RESET CHANNEL potvrdil, že data synchronizace byla ztracena, a povolil kanálu pokračovat ve spouštění.

Ve správci front příjemce musí být nastaven atribut **IgnoreSeqNumberMismatch** .

V podstatě tento atribut provádí příkaz resetu kanálu na přijímacím kanálu.

Tento atribut řídí způsob, jakým správce front zpracovává neshodu pořadových čísel během spouštění kanálu, a to pomocí následujících hodnot:

NO
Během resynchronizace kanálu se kontrolují pořadová čísla kanálu. Pokud se oba MCA neshodují na stejném pořadovém čísle, bude ohlášena chybová zpráva AMQ9526 a kanál se nespustí.

YES
Během resynchronizace kanálu jsou kontrolována pořadová čísla kanálu, ale pokud se oba MCA neshodují na stejném pořadovém čísle, bude ohlášena varovná zpráva AMQ9703 a spuštění kanálu bude pokračovat. Tato hodnota atributu by neměla být za normálních okolností potřebná.

Když je známo, že data synchronizace byla ztracena, například během zotavení z havárie, tato volba se vyhne nutnosti ručně potvrdit každou neshodu pořadových čísel. Uvedení této hodnoty má podobný efekt jako administrátor automaticky vydávající **RESET CHANNEL** jako odpověď na každou neshodu pořadových čísel.

ChlauthIgnoreUserCase = N (výchozí) | Y

Umožňuje správci front provádět shodu jména uživatele v pravidlech CHLAUTH bez rozlišování malých a velkých písmen. Tato volba umožňuje:

- CLNTUSER v pravidlech CHLAUTH TYPE (USERMAP), která se neshodují s velikostí písmen
- USERLIST v pravidlech CHLAUTH TYPE (BLOCKUSER), která se neshodují s velikostí písmen-bez ohledu na velikost písmen

Platné hodnoty pro **ChlauthIgnoreUserCase** jsou následující hodnoty:

N

Pravidla ověřování kanálu se pokusí porovnat identifikaci uživatele klienta s rozlišováním malých a velkých písmen, například pravidlo určující CLNTUSER ('Fred') se neshoduje s 'fred' nebo 'FRED', bude se shodovat pouze s identifikátorem uživatele 'Fred'. Toto je výchozí hodnota.

Y

Pravidla ověřování kanálu se pokusí porovnat identifikaci uživatele klienta s rozlišováním malých a velkých písmen, například pravidlo ověřování kanálu s TYPE (USERMAP) nebo TYPE (USERBLOCK) určujícím CLNTUSER ('Fred') se bude shodovat s jakoukoli variantou rozlišování velkých a malých písmen, například identifikátory uživatelů 'Fred', 'FRED' a 'fred' se shodují.

Všimněte si, že při ignorování velkých a malých písmen identifikátorů uživatelů při porovnávání pravidel ověřování kanálu je možné, aby se shodovala více než jedna pravidla. Pokud k tomu dojde, pravidlo, které se shoduje, je nedefinované. Například s následujícími pravidly, pokud se uživatel 'fred' připojí ke správci front prostřednictvím kanálu CLIENT, mohou být namapovány na 'mquser1' nebo 'mquser2':

```
SET CHLAUTH('CLIENT') TYPE(USERMAP) CLNTUSER('fred') USERSRC(MAP) MCAUSER('mquser1')
SET CHLAUTH('CLIENT') TYPE(USERMAP) CLNTUSER('FRED') USERSRC(MAP) MCAUSER('mquser2')
```

Chcete-li se vyvarovat jakékoli nejistotě při použití `ChlauthIgnoreUserCase=Y`, vyvarujte se definování pravidel CHLAUTH, která by se překrývala a vedla k odlišnému chování při použití shody bez rozlišování velkých a malých písmen.

ChlauthIssueVarování = y

Tento atribut nastavte, chcete-li, aby byla při nastavení atributu WARN = YES v příkazu **SET CHLAUTH** generována zpráva AMQ9787 .

Příklad stanza

```
Channels:
   MaxChannels=200
   MaxActiveChannels=100
   MQIBindType=STANDARD
   PipelineLength=2
```

Související pojmy

“Stavy kanálů” na stránce 220

Kanál může být v jednom z mnoha stavů kdykoli. Některé státy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

Multi Sekce připojení souboru qm.ini

Sekce Připojení definuje výchozí typ vazby.

K určení výchozího typu vazby použijte sekci Připojení v souboru `qm.ini` .

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer `Extended` .

Poznámka: Pokud potřebujete sekci Připojení, musíte ji vytvořit.

DefaultBindTyp = SHARED (výchozí) |ISOLATED
Je-li parametr **DefaultBindType** nastaven na hodnotu `ISOLATED`, aplikace a správce front jsou spouštěny v samostatných procesech a nejsou mezi nimi sdíleny žádné prostředky.

Je-li parametr **DefaultBindType** nastaven na hodnotu SHARED, aplikace a správce front se spouštějí v samostatných procesech, ale některé prostředky jsou mezi nimi sdíleny.

Výchozí hodnota je SHARED.

Upozornění: DefaultBindType platí pro všechna volání MQCONN a všechna volání MQCONNX s volbou MQCNO_STANDARD_BINDING.

Změna parametru **DefaultBindType** může způsobit snížení výkonu některých aplikací.

Příklad stanza

```
Connection:
  DefaultBindType=SHARED
```

Multi Protokolování diagnostických zpráv

Protokoly diagnostických zpráv produktu IBM MQ jsou mechanizmem, který umožňuje různým komponentám systému IBM MQ hlásit diagnostické zprávy související s konfigurací produktu IBM MQ a změnami a problémy stavu běhového prostředí.

Tyto protokoly jsou někdy označovány jako IBM MQ *protokoly chyb*, ale vždy obsahovaly informace IBM MQ a varovné zprávy, stejně jako chybové zprávy. Tři primární komponenty produktu IBM MQ , které se hlásí k těmto protokolům, jsou:

- Správci front
- IBM MQ Klienti
- Zbytek systému IBM MQ

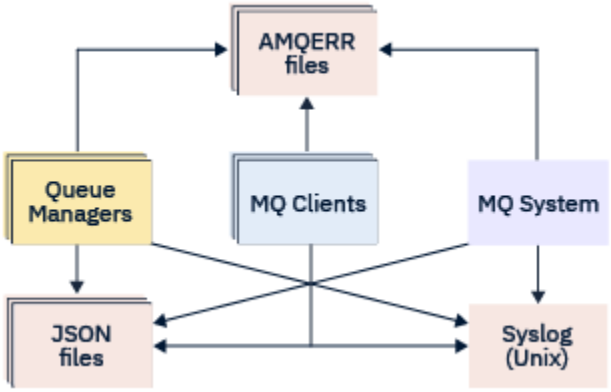
Produkt IBM MQ podporuje vytváření sestav diagnostických zpráv prostřednictvím řady různých metod známých jako *služby diagnostických zpráv*, což umožňuje přizpůsobený přístup k zaznamenávání a využívání těchto informací:

- Soubory protokolu AMQERRnn
- Soubory protokolu ve formátu JSON
- AIX Syslog ve formátu JSON

Výstup JSON podle IBM MQ je formátován jako objekty JSON s jedním řádkem, takže každý jednotlivý řádek protokolu JSON nebo záznam Syslog představuje platný objekt JSON. Protokol jako celek není zapouzdřen jako jeden objekt JSON.

Následující obrázek ukazuje, že správci front, klienti IBM MQ a systém IBM MQ mohou *všechny* zprávy diagnostiky hlásit pomocí popsaných metod.

Obrázek 5. Jak různé části produktu IBM MQ mohou hlásit diagnostické zprávy



Jak jsou nakonfigurovány protokoly diagnostiky IBM MQ :

Diagnostické protokoly jsou definovány a upraveny pomocí sekcí v souboru `qm.ini` , které jsou specifické pro komponentu IBM MQ , která je vyžaduje. Každý jedinečný koncový bod protokolování je definován pod vlastním záhlavím sekce v souboru ini spolu s veškerými přizpůsobeními, která jsou v něm definována. Přizpůsobení mohou zahrnovat:

- Velikost souborů protokolu, které se mají zalomit, než dojde k přetočení; nelze použít pro Syslog
- Jakékoli filtrování na základě závažnosti zpráv protokolu a
- Všechny specifické kódy zpráv, které mají být potlačeny.

Produkt IBM MQ lze nakonfigurovat tak, aby zapisoval do libovolných nebo všech tří typů koncových bodů protokolování, což umožňuje, aby konkrétní sekce protokolu plnily určité role. Podobně lze definovat více souborových služeb. Příklad:

- Formát JSON usnadňuje analýzu prostřednictvím automatizovaných nástrojů v lokálních a cloudových prostředích.
- Výstup syslog umožňuje komponentám IBM MQ integrovat diagnostické informace do společného umístění protokolování operačního systému v souladu s ostatními produkty v systému.
- Koncové body protokolu jsou filtrovány na základě závažnosti, což umožňuje určitým souborům protokolu zaznamenávat například pouze závažné chyby v systému.

Bez ohledu na styl konfigurovaného protokolování diagnostiky se soubory tradiční diagnostiky uložené v adresáři systémového protokolu IBM MQ (`/var/mqm/errors/AMQERRnn.log`) a ve specifickém adresáři protokolu správce front (`/var/mqm/qmgrs/<qmgr_name>/errors/AMQERRnn.log`) vždy zapisují kromě jiné použité konfigurace protokolování.

Pouze pro správce front lze volitelnou konfiguraci těchto povinných protokolů provést zadáním atributů “Sekce služby diagnostických zpráv” na stránce 123.

Různé oblasti stanzy

Další sekce lze použít na různé oblasti produktu IBM MQ.

Správce front (qm.ini)
Platí pro zprávu protokolu generovanou správcem front

Systém (mqs.ini)
Platí pro zprávy protokolu generované systémem. Tato volba není specifická pro správce front, s výjimkou případů, kdy správce front nemůže přistupovat k vlastním protokolům nebo do nich zapisovat.

Šablony (mqs.ini)
Jedna nebo více sekcí jako šablony, které jsou při vytvoření správce front zkopírovány do adresáře `qm.ini` .

Klient (mqclient.ini)
Platí pro operace klienta, například **runmqsc** v režimu klienta pro vzdáleného správce front.

Převod mezi protokoly ve formátu JSON a tradičně formátovanými protokoly

Příkaz mqrc byl rozšířen tak, aby umožňoval řadu převodů mezi protokoly JSON a tradičně formátovanými protokoly a mezi různými jazyky.

Související odkazy
"Sekce služby diagnostických zpráv" na stránce 123
Dostupné volby služby diagnostických zpráv umožňují přizpůsobit protokolování diagnostiky produktu IBM MQ tak, aby výstup protokolu mohl být směrován na různé koncové body protokolu z různých komponent produktu IBM MQ.

"Sekce QMErrorLog" na stránce 122
Sekci protokolu chyb správce front QMErrorLog v souboru `qm.ini` použijete k přizpůsobení operací a obsahu protokolů chyb IBM MQ .

"Služby diagnostických zpráv" na stránce 126
Lze definovat následující diagnostické služby zpráv a jejich atributy specifické pro služby, které jsou uvedeny v sekcích DiagnosticSystemMessages, DiagnosticMessages a DiagnosticMessagesTemplate konfiguračních souborů:

Multi *Sekce QMErrorLog*

Sekci protokolu chyb správce front QMErrorLog v souboru `qm.ini` použijete k přizpůsobení operací a obsahu protokolů chyb IBM MQ .

Služba QMErrorLog je tradiční služba protokolování diagnostiky IBM MQ používaná k výstupu diagnostických zpráv týkajících se správce front. Služba QMErrorLog běží nepřetržitě a nelze ji vypnout, ale lze ji do určité míry upravit.

Sekci QMErrorLog v souboru `qm.ini` můžete použít k vyloučení určitých zpráv z zápisu do protokolu chyb správce front. Můžete také potlačit zápis zpráv do protokolu chyb pro daný časový interval.

Windows Linux Alternativně můžete namísto přímé úpravy souboru `qm.ini` použít stránku vlastností rozšířeného správce front v souboru IBM MQ Explorer k vyloučení a potlačení zpráv pomocí atributů **Vyloučené zprávy**, **Potlačené zprávy** a **Interval potlačených zpráv** .

Upozornění:

- Windows Produkt IBM MQ Explorer můžete použít k provedení změn pouze v případě, že používáte lokálního správce front na platformě Windows .
- Sekce QMErrorLog není použitelná pro konfigurační soubor systému IBM MQ , `mqs.ini`nebo konfigurační soubor klienta, obecně nazvaný `mqclient.ini`.

Následující atributy lze zahrnout do sekce QMErrorLog :

ErrorLogVelikost = *maxsize*
Určuje velikost protokolu chyb správce front, který je zkopírován do zálohy. Hodnota *maxsize* musí být v rozsahu 32768 až 2147483648 bajtů. Není-li parametr **ErrorLogSize** uveden, použije se výchozí hodnota 33554432 bajtů (32 MB).

Pomocí tohoto atributu můžete v případě potřeby snížit maximální velikost zpět na předchozí maximum 2 MB.

Velikost protokolu můžete nastavit pomocí proměnné prostředí **MQMAXERRORLOGSIZE** .

ExcludeMessage= *msgIds*
Určuje zprávy, které nemají být zapsány do protokolu chyb správce front.

Další informace viz ExcludeMessage v "Sekce služby diagnostických zpráv" na stránce 123 .

SuppressMessage= *msgIds*
Určuje zprávy, které jsou zapsány do protokolu chyb správce front pouze jednou v určeném časovém intervalu. Pokud je stejné ID zprávy uvedeno jak v `SuppressMessage` , tak i v `ExcludeMessage`, je zpráva vyloučena.

Tuto volbu nelze použít pro služby diagnostických zpráv definované v souboru `mqclient.ini`. Další informace viz SuppressMessage v části “Sekce služby diagnostických zpráv” na stránce 123.

SuppressInterval= *délka*
Určuje časový interval v sekundách, ve kterém jsou zprávy určené v poli `SuppressMessage` zapisovány do protokolu chyb správce front pouze jednou. *length* musí být v rozsahu 1 až 86400 sekund. Není-li zadána hodnota `SuppressInterval` , bude použita výchozí hodnota 30 sekund.

Příklad stanza

```
QMErrorLog:
   ErrorLogSize=262144
   ExcludeMessage=7234
   SuppressMessage=9001,9002,9202
   SuppressInterval=30
```

Související pojmy

“Konfigurační soubory správce front, qm.ini” na stránce 97
Konfigurační soubor správce front `qm.ini`obsahuje informace týkající se konkrétního správce front. Atributy, které můžete použít k úpravě konfigurace jednotlivého správce front, přepíší veškerá nastavení pro produkt IBM MQ.

Související odkazy

“Sekce služby diagnostických zpráv” na stránce 123
Dostupné volby služby diagnostických zpráv umožňují přizpůsobit protokolování diagnostiky produktu IBM MQ tak, aby výstup protokolu mohl být směrován na různé koncové body protokolu z různých komponent produktu IBM MQ.

Multi *Sekce služby diagnostických zpráv*

Dostupné volby služby diagnostických zpráv umožňují přizpůsobit protokolování diagnostiky produktu IBM MQ tak, aby výstup protokolu mohl být směrován na různé koncové body protokolu z různých komponent produktu IBM MQ.

Povolíte další služby diagnostiky zpráv pomocí sekce s jedním z následujících názvů:

- **`DiagnosticSystemMessages`**

  Definuje služby používané při generování diagnostické zprávy, která přejde do systémového protokolu chyb. Platné v souborech `mqs.ini` nebo `mqclient.ini` .

  Klientské aplikace používají sekci **`DiagnosticSystemMessages`** v souboru mqclient.ini a v souboru mqs.iniřídí sekce **`DiagnosticSystemMessages`** zprávy pro serverovou aplikaci, která nemá kontext správce front.

  Je možné konfigurovat správce front a aplikace, které dodatečně zapisují všechny zprávy do služby syslog.

- **`DiagnosticMessages`**

  Definuje služby používané při generování diagnostické zprávy, která přejde do protokolu chyb správce front. Platné pouze v souboru `qm.ini` .

- **`DiagnosticMessagesTemplate`**

  Sekce zkopírovaná ze souboru `mqs.ini` do souboru **`DiagnosticMessages`** v souboru `qm.ini` při vytvoření správce front.

Chcete-li zobrazit diagnostické zprávy, použijte příkaz mqrc .

Atributy sekcí

Upozornění: `Službaa` název sekce jsou povinné.

name= < stanzaname>
Název stanzy. Hodnota musí být v souboru ini jedinečná.

Service = *typ služby*

Tento atribut definuje službu, kde název služby nerozlišuje malá a velká písmena, která je povolena touto sekcí.

Chcete-li například povolit `syslog` jako další službu, zadejte následující:

```
Service=syslog
```

Viz “Služby diagnostických zpráv” na stránce 126 a jejich specifické atributy, které jsou k dispozici pro použití s oddíly diagnostické služby zpráv.

Do sekcí můžete přidat následující volitelné atributy:

- ExcludeMessage
- SuppressMessage
- SuppressInterval
- “Závažnosti” na stránce 125

ExcludeMessage= *msgIds*
Určuje zprávy, které nemají být zapsány do protokolu chyb správce front. Pokud je systém IBM MQ intenzivně využíván a mnoho kanálů se zastavuje a spouští, odešle se velký počet informačních zpráv do konzoly z/OS a do protokolu tištěné kopie. Správce mostu a vyrovnávací paměti IBM MQ - IMS může také vytvořit velký počet informačních zpráv, takže vyloučení zpráv vám zabrání v přijímání velkého počtu zpráv, pokud je požadujete. *msgIds* obsahuje seznam ID zpráv oddělených čárkami z následujících položek:

5211-Byla překročena maximální délka názvu vlastnosti.
5973-Odběr distribuovaného publikování/odběru byl zablokován
5974-Distribuované publikování/odběr blokováno
6254-Systému se nepodařilo dynamicky načíst sdílenou knihovnu.
IBM i 7163 - Zpráva o spuštění úlohy (pouze IBM i).
7234 - Počet načtených zpráv.
8245-Entita nemá dostatečná oprávnění k zobrazení objektu
9001 - Program kanálu byl standardně ukončen.
9002 - Program kanálu byl spuštěn.
9202 - Vzdálený hostitel je nedostupný.
9208-Chyba při příjmu od hostitele
9209-Spojení uzavřeno
9228-Nelze spustit odpovídací modul kanálu
9489-Byl překročen maximální limit instancí SVRCONN
9490-Byl překročen maximální počet instancí SVRCONN na klienta
9508-Nelze se připojit ke správci front
9524 - Vzdálený správce front je nedostupný.
9528 - Zavření kanálu vyžadované uživatelem.
9545-Interval odpojení vypršel
9558-Vzdálený kanál není k dispozici
9637-kanálu chybí certifikát
9776-Kanál byl blokován ID uživatele
9777-Kanál byl zablokován mapou NOACCESS

9782-Připojení bylo zablokováno adresou
9999 - Program kanálu byl ukončen nestandardně.

SuppressMessage= *msgIds*
Určuje zprávy, které jsou zapsány do protokolu chyb správce front pouze jednou v určeném časovém intervalu. Pokud je systém IBM MQ intenzivně využíván a mnoho kanálů se zastavuje a spouští, odešle se velký počet informačních zpráv do konzoly z/OS a do protokolu tištěné kopie. Správce mostů a vyrovnávacích pamětí IBM MQ - IMS může také vytvářet velký počet informačních zpráv, takže potlačení zpráv vám v případě potřeby zabrání v přijetí určitého počtu opakujících se zpráv. Časový interval je určen parametrem `SuppressInterval`. *msgIds* obsahuje seznam identifikátorů zpráv oddělených čárkami z následujících položek:

5211-Byla překročena maximální délka názvu vlastnosti.
5973-Odběr distribuovaného publikování/odběru byl zablokován
5974-Distribuované publikování/odběr blokováno
6254-Systému se nepodařilo dynamicky načíst sdílenou knihovnu.
IBM i 7163 - Zpráva o spuštění úlohy (pouze IBM i).
7234 - Počet načtených zpráv.
8245-Entita nemá dostatečná oprávnění k zobrazení objektu
9001 - Program kanálu byl standardně ukončen.
9002 - Program kanálu byl spuštěn.
9202 - Vzdálený hostitel je nedostupný.
9208-Chyba při příjmu od hostitele
9209-Spojení uzavřeno
9228-Nelze spustit odpovídací modul kanálu
9489-Byl překročen maximální limit instancí SVRCONN
9490-Byl překročen maximální počet instancí SVRCONN na klienta
9508-Nelze se připojit ke správci front
9524 - Vzdálený správce front je nedostupný.
9528 - Zavření kanálu vyžadované uživatelem.
9545-Interval odpojení vypršel
9558-Vzdálený kanál není k dispozici
9637-kanálu chybí certifikát
9776-Kanál byl blokován ID uživatele
9777-Kanál byl zablokován mapou NOACCESS
9782-Připojení bylo zablokováno adresou
9999 - Program kanálu byl ukončen nestandardně.

Pokud je stejné ID zprávy uvedeno jak v `SuppressMessage` , tak v `ExcludeMessage`, je zpráva vyloučena.

Tuto volbu nelze použít pro služby diagnostických zpráv definované v souboru `MQ client.ini`.

SuppressInterval= *délka*
Určuje časový interval v sekundách, ve kterém jsou zprávy určené v souboru **SuppressMessage** zapisovány do protokolu chyb správce front pouze jednou. *length* musí být v rozsahu 1-86400 sekund. Není-li parametr **`SuppressInterval`** uveden, použije se výchozí hodnota 30 sekund.

Závažnosti
Čárkami oddělený seznam úrovní závažnosti, kde název úrovně závažnosti nerozlišuje velká a malá písmena. Přípustné hodnoty jsou:

- I (nebo Informace nebo 0)
- W (nebo Varování nebo 10)
- E (nebo Chyba nebo 20 a 30)
- S (nebo Stop nebo 40)

- T (nebo Systém nebo 50)

Notes:

1. Výchozí hodnota je `all` .
2. Službě jsou prezentovány pouze zprávy ve vybraných úrovních závažnosti.

   Případně můžete použít znak plus (+), který zobrazí uvedenou úroveň chyby, a všechny vyšší úrovně. Chcete-li například zobrazit všechny chyby:

```
Severities=E+
```

Související odkazy

“Sekce QMErrorLog” na stránce 122
Sekci protokolu chyb správce front QMErrorLog v souboru `qm.ini` použijete k přizpůsobení operací a obsahu protokolů chyb IBM MQ .

“Služby diagnostických zpráv” na stránce 126
Lze definovat následující diagnostické služby zpráv a jejich atributy specifické pro služby, které jsou uvedeny v sekcích DiagnosticSystemMessages, DiagnosticMessages a DiagnosticMessagesTemplate konfiguračních souborů:

Multi *Služby diagnostických zpráv*

Lze definovat následující diagnostické služby zpráv a jejich atributy specifické pro služby, které jsou uvedeny v sekcích DiagnosticSystemMessages, DiagnosticMessages a DiagnosticMessagesTemplate konfiguračních souborů:

Jsou definovány následující služby diagnostických zpráv:

Soubor

Tato služba odesílá nefiltrované zprávy do souboru podobným způsobem jako služba QMErrorLog . V závislosti na zadaném souboru **Format**se použije buď existující textový formát, nebo uvedený formát JSON. Standardně existují tři soubory s názvem `AMQERR01.LOG`, `AMQERR02.LOG`a `AMQERR03.LOG` nebo `AMQERR01.json`, `AMQERR02.json`a `AMQERR03.json`, v závislosti na vlastnosti **Format** , a tyto přetočení založené na nakonfigurované velikosti.

Následující atributy jsou podporovány pouze v sekci Soubor:

FilePath

Cesta, kam se zapisují soubory protokolu. Výchozí umístění je stejné jako umístění souborů `AMQERR01.log` , tj. systém nebo správce front. Cesta musí být absolutní, ale může obsahovat vyměnitelné vložky. Příklad:

+ MQ_Q_MGR_DATA_PATH +

Úplná cesta k nadřízenému adresáři diagnostických zpráv správce front. Výchozí hodnoty jsou:

- Linux AIX Na platformách AIX and Linux : `/var/mqm/qmgrs/<QM_name>`
- Windows v systému Windows, `C:\Program Data\IBM\MQ\qmgrs\<QM_name>`

+ MQ_DATA_PATH +

Úplná cesta k nadřízenému adresáři zpráv diagnostiky systému. Výchozí hodnoty jsou:

- Linux AIX Na platformách AIX and Linux :`/var/mqm`
- Windows V systému Windows: `C:\Program Data\IBM\MQ`

Tuto cestu musíte vytvořit s odpovídajícími oprávněními, pokud nepoužívá existující adresář chyb.

FilePrefix

Předpona souborů protokolu. Předvolba je AMQERR.

FileSize
Velikost, při které se protokol přetočí. Výchozí hodnota je 32MB, stejně jako u vlastnosti **ErrorLogSize** prvku "Sekce QMErrorLog" na stránce 122, který je sémanticky identický.

Poznámka: Vlastnost **ErrorLogSize** se vztahuje pouze na výchozí službu protokolu chyb, nikoli na vlastní diagnostické služby.

Velikost protokolu můžete nastavit pomocí proměnné prostředí **MQMAXERRORLOGSIZE** .

Format
Formát souboru. Hodnota může být buď *text* (pro další služby stylu QMErrorLog), nebo *json*, což je předvolba.

Přípona souboru je buď `.LOG` , nebo `.json` na základě nastavení tohoto atributu.

Upravte například soubor `qm.ini` správce front a přidejte následující sekci:

```
DiagnosticMessages:
   Service = File
   Name = JSONLogs
   Format = json
   FilePrefix = AMQERR
```

Po restartování bude mít správce front soubory `AMQERR0x.json` ve svém adresáři ERRORS.

Můžete definovat více souborové služby. To umožňuje konfiguraci, jak je uvedeno v následujících příkladech, kde jsou zprávy různých značek rozděleny na různé sady protokolů:

```
DiagnosticMessages:
  Name=ErrorsToFile
  Service=File
  Severities=E+
  FilePrefix=OnlyErrors

DiagnosticMessages:
  Name=NonErrorstoFile
  Service=File
  Severities=1 W
  FilePrefix=Information
```

Linux AIX **Systémový protokol**

Služba Syslog není k dispozici na systému Windows nebo IBM i

Můžete definovat pouze jednu službu Syslog a služba Syslog odešle nefiltrované zprávy do syslog pomocí specifikace diagnostických zpráv formátu JSON . Informace se přidají do syslog v pořadí zobrazeném v tabulce, počínaje msgID a vložením.

Závažnost zprávy je mapována na úroveň syslog následujícím způsobem:

Tabulka 12. Mapování závažnosti zprávy na úroveň systémového protokolu

Závažnost	**Úroveň**
0	LOG_INFO
10	Log_VAROVÁNÍ
20	Log_ERR
30	Log_ERR
40	LOG_VÝSTRAHA
50	LOG_VÝSTRAHA

Následující atribut je podporován pouze v sekci syslog:

Ident
Definuje hodnotu **ident** přidruženou k položkám syslog. Výchozí hodnota je *ibm-mq*.

Následující příklad ukazuje chybové zprávy odesílané do Syslog:

```
DiagnosticMessages:
  Name=ErrorsToSyslog
  Ident=mq
  Service=Syslog
  Severities=E+
```

Další informace o atributech generické sekce viz “Sekce služby diagnostických zpráv” na stránce 123 .

Notes:

1. Pouze pro službu Soubor můžete mít více sekcí, každá s jiným názvem. Použije se pouze definice používající konečné jméno v posloupnosti.
2. Změny hodnoty sekce se projeví až po restartování správce front.

Multi Sekce ExitPath souboru qm.ini

Sekce ExitPath uvádí cestu pro uživatelské programy v systému správce front.

Pomocí sekce `ExitPath` v souboru `qm.ini` určete cestu pro programy uživatelských procedur v systému správce front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer `Exits` .

ExitsDefaultCesta = ***řetězec***
Atribut cesty ExitsDefaultuvádí umístění:

- 32bitové uživatelské procedury kanálu pro klienty
- 32bitové uživatelské procedury kanálu a uživatelské procedury převodu dat pro servery
- Nekvalifikované soubory načtení přepínače XA

ExitsDefaultPath64= ***řetězec***
Atribut ExitsDefaultPath64 určuje umístění:

- 64bitové uživatelské procedury kanálu pro klienty
- 64bitové uživatelské procedury kanálu a uživatelské procedury převodu dat pro servery
- Nekvalifikované soubory načtení přepínače XA

Příklad stanza

```
ExitPath:
   ExitsDefaultPath=/var/mqm/exits
   ExitsDefaultPath64=/var/mqm/exits64
```

Multi ExitPropertiesLokální sekce souboru qm.ini

Lokální sekce ExitPropertiesuvádí informace o vlastnostech ukončení ve správci front.

Chcete-li zadat informace o vlastnostech ukončení ve správci front, použijte lokální sekci ExitPropertiesv souboru `qm.ini` .

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front klastru IBM MQ Explorer .

Windows Případně v systému Windows můžete tyto informace zadat pomocí příkazu **amqmdain** .

Standardně je toto nastavení zděděno z atributu **CLWLMode** v sekci ExitProperties konfigurace pro celý počítač (popsáno v tématu “ExitProperties sekce souboru mqs.ini” na stránce 92). Toto nastavení změňte pouze v případě, že chcete konfigurovat tohoto správce front jiným způsobem. Tuto hodnotu lze pro jednotlivé správce front přepsat pomocí atributu režimu pracovní zátěže klastru na stránce vlastností správce front klastru.

Sekci ExitProperties v souboru `mqs.ini` použijte k určení voleb konfigurace, které používají uživatelské programy správce front.

Windows Linux Případně na systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `Extended` IBM MQ .

CLWLMode = SAFE (výchozí) | RYCHLE
Uživatelská procedura pracovní zátěže klastru (CLWL) vám umožňuje určit, která fronta klastru se má v klastru otevřít v reakci na volání MQI (například `MQOPEN`, `MQPUT`). Uživatelská procedura CLWL se spustí buď v režimu FAST, nebo v režimu SAFE v závislosti na hodnotě zadané v atributu **CLWLMode** . Pokud vynecháte atribut **CLWLMode** , uživatelská procedura pracovní zátěže klastru se spustí v režimu SAFE.

Bezpečný
Spusťte uživatelskou proceduru CLWL v odděleném procesu od správce front. Toto nastavení je výchozí.

Pokud při spuštění v režimu SAFE dojde k problému s uživatelskou procedurou CLWL, dojde k následujícím událostem:

- Proces serveru CLWL (amqzlwa0) selže.
- Správce front restartuje proces serveru CLWL.
- Chyba je vám nahlášena v protokolu chyb. Pokud probíhá volání MQI, obdržíte oznámení ve formě návratového kódu.

Integrita správce front je zachována.

Poznámka: Spuštění uživatelské procedury CLWL v samostatném 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 procesů přidruženým ke spuštění v režimu SAFE, ale učiníte tak na úkor integrity správce front. Uživatelskou proceduru CLWL byste měli spustit pouze v režimu FAST, pokud jste přesvědčeni, že s uživatelskou procedurou CLWL nejsou žádné problémy, a jste obzvláště znepokojeni výkonem.

Pokud dojde k problému při spuštění uživatelské procedury CLWL v režimu FAST, dojde k selhání správce front a riskujete ohrožení integrity správce front.

Příklad stanza

```
ExitPropertiesLocal:
      CLWLMode=SAFE
```

Linux IBM i AIX Sekce systému souborů souboru qm.ini

Sekce Systém souborů určuje, zda mají oprávnění nastavená pro protokoly chyb správce front zůstat beze změny nebo zda mají být změněna zpět na výchozí hodnoty.

Ve většině případů se očekává, že výchozí oprávnění nastavená pro soubory protokolu chyb budou užitečná, a proto není nutné, aby je většina administrátorů produktu IBM MQ měnila.

Administrátor produktu IBM MQ však může chtít změnit oprávnění pro své soubory protokolu chyb. V takovém případě by měl nastavit volbu `Filesystem` stanza **ValidateAuth**=*No*, což způsobí, že správce front ponechá oprávnění nezměněná.

Výchozí chování (bez hodnoty **ValidateAuth**=*Ne*) spočívá v tom, že správce front zkontroluje oprávnění k souborům protokolů chyb správce front a změní je zpět na výchozí hodnoty. K této kontrole může dojít kdykoli, a to i během operace ukončení nebo spuštění správce front.

Příklad stanza

```
Filesystem:
      ValidateAuth=No
```

Multi Sekce protokolu souboru qm.ini

Sekce Protokol uvádí informace o protokolování ve správci front.

Sekci Protokol v souboru `qm.ini` použijte k uvedení informací o protokolování ve správci front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer **Správce front protokolu** .

Standardně jsou tato nastavení zděděna z nastavení, která jsou určena pro výchozí nastavení protokolu pro správce front (viz “Sekce LogDefaults souboru mqs.ini” na stránce 93). Tato nastavení změňte pouze v případě, že chcete konfigurovat tohoto správce front jiným způsobem.

Další informace o výpočtu velikosti protokolu viz “Výpočet velikosti protokolu” na stránce 628.

Poznámka: Omezení uvedená v následujícím seznamu parametrů jsou nastavena pomocí IBM MQ. Omezení operačního systému mohou snížit maximální možnou velikost protokolu.

LogPrimaryFiles = 3 (výchozí) |*2-254* (Windows) |*2-510* (systémy AIX and Linux)
Soubory protokolu přidělené při vytvoření správce front.

Minimální počet primárních souborů protokolu, které můžete mít, je 2 a maximum je 254 v systému Windowsnebo 510 v systémech AIX and Linux . Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systémech AIX 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 se však neprojeví, dokud nebude správce front restartován a efekt nemusí být okamžitý.

LogSecondaryFiles = 2 (výchozí) |*1-253* (Windows) |*1-509* (systémy AIX and Linux)
Soubory protokolu přidělené při vyčerpání primárních souborů.

Minimální počet sekundárních souborů protokolu je 1 a maximum je 253 na systémech Windowsnebo 509 na systémech AIX and Linux . Výchozí číslo je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systémech AIX and Linux a nesmí být menší než 3.

Hodnota je prozkoumána při spuštění správce front. Tuto hodnotu můžete změnit, ale změny se neprojeví, dokud nebude správce front restartován, a i tak nemusí být efekt okamžitý.

LogFilePočet stránek = *number*
Data protokolu jsou uložena v řadě souborů nazývaných soubory protokolu. Velikost souboru protokolu je určena v jednotkách stránek o velikosti 4 kB.

Výchozí počet stránek souboru protokolu je 4096 a velikost souboru protokolu je 16 MB.

Na systémech AIX and Linux je minimální počet stránek souboru protokolu 64 a na systému Windows je minimální počet stránek souboru protokolu 32; v obou případech je maximální počet 65 535.

Poznámka: Velikost souborů protokolu, které jsou určeny během vytváření správce front, nelze pro správce front změnit.

LogType = CIRCULAR (výchozí nastavení) | LINEAR| REPLIKOVÁNO
Typ protokolování, který má používat správce front. Výchozí hodnota je CIRCULAR. Další informace o vytvoření správce front s požadovaným typem protokolování naleznete v popisu atributu **LogType** v části "Sekce LogDefaults souboru mqs.ini" na stránce 93.

KRUHOVÉ
Spusťte obnovu po restartu pomocí protokolu pro odvolání transakcí, které probíhaly při zastavení systému.

Podrobnější vysvětlení kruhového protokolování naleznete v části "Typy protokolování" na stránce 623 .

Lineární
Jak pro obnovu po restartu, tak pro obnovu po předání (vytváření ztracených nebo poškozených dat přehráváním obsahu protokolu).

Podrobnější vysvětlení lineárního protokolování naleznete v části "Typy protokolování" na stránce 623 .

CP4I **Replikováno**
Používá skupina Nativní HA k replikaci dat protokolu z aktivní instance do instancí repliky.

Podrobnější vysvětlení replikovaného protokolování naleznete v části "Typy protokolování" na stránce 623 .

Poznámka: Položku **LogType** správce front nelze změnit úpravou tohoto atributu v souboru `qm.ini` . Chcete-li změnit **LogType** správce front, musíte použít příkaz **migmqlog** .

LogBufferPages=0 (výchozí) |*0-4096*
Množství paměti přidělené záznamům vyrovnávací paměti pro zápis, určující velikost vyrovnávacích pamětí v jednotkách 4kB stránek.

Minimální počet stránek vyrovnávací paměti je 18 a maximální je 4096. Větší vyrovnávací paměti přispívají k vyšší propustnosti, zvláště velkých zpráv.

Jestliže uvedete 0 (předvolba), správce front vybere velikost.

Zadáte-li číslo v rozsahu 1 až 17, bude pro správce front použita výchozí hodnota 18 (72 kB). Zadáte-li číslo v rozsahu 18 až 4096, správce front použije zadané číslo k nastavení množství přidělené paměti.

Hodnota je prozkoumána při spuštění správce front. Hodnotu lze zvýšit nebo snížit v uvedených mezích. Změna hodnoty se však projeví až po příštím spuštění správce front.

LogPath= *název_adresáře*
Adresář, ve kterém jsou umístěny soubory protokolu pro správce front. Musí existovat na lokálním zařízení, do kterého může správce front zapisovat, a pokud možno na jiné jednotce než ve frontách zpráv. Uvedení jiné jednotky poskytuje přidanou ochranu v případě selhání systému.

Výchozí nastavení je:

- Windows `C:\ProgramData\IBM\MQ\log` v souboru Windows.
- Linux AIX `/var/mqm/log` v systémech AIX and Linux .

Název adresáře můžete zadat v příkazu **crtmqm** pomocí příznaku **-ld** . Při vytvoření správce front je v adresáři správce front vytvořen také adresář, který slouží k uchování souborů protokolu. Název tohoto adresáře je založen na názvu správce front. Tím zajistíte, že cesta k souboru protokolu bude jedinečná a že bude v souladu se všemi omezeními délky názvů adresářů.

Pokud neuvedete `-ld` v příkazu **crtmqm** , použije se hodnota atributu **LogDefaultPath** .

Linux AIX Na systémech AIX and Linux musí mít ID uživatele mqm a skupina mqm úplná oprávnění k souborům protokolu. Pokud změníte umístění těchto souborů, musíte tato

oprávnění udělit sami. Toto není vyžadováno, pokud jsou soubory protokolu ve výchozích umístěních dodaných s produktem.

LogWriteIntegrity =SingleWrite|DoubleWrite|TripleWrite (výchozí)
Metoda, kterou modul protokolování používá k spolehlivému zápisu záznamů protokolu.

TripleWrite (výchozí)

Všimněte si, že lze vybrat volbu DoubleWrite. Když tak ale uděláte, systém to interpretuje jako volbu TripleWrite.

SingleWrite
Měli byste použít SingleWrite, pouze pokud systém souborů a zařízení hostující protokol pro zotavení IBM MQ výslovně zaručují atomicitu 4KB zápisů.

Když se tedy zápis 4kB stránky nezdaří z nějakého důvodu, jsou možné jen dva stavy: před obrazem nebo po obrazu. Žádný mezistav by neměl být možný.

Poznámka: Pokud je ve vaší trvalé pracovní zátěži dostatečná souběžnost, existuje minimální potenciální přínos při nastavování jiné než výchozí hodnoty TripleWrite.

Další informace viz téma "LogWriteIntegrita-použití SingleWrite nebo TripleWrite" na stránce 133.

LogManagement = Manual (výchozí) | Automaticky | Archivovat
Metoda používaná ke správě oblastí protokolu, a to buď ručně, nebo pomocí správce front. Výchozí hodnota je Ruční.

Atribut se použije pouze v případě, že **LogType** je LINEAR.

Změníte-li hodnotu **LogManagement**, změna se neprojeví, dokud nebude správce front restartován.

Pokud je pro atribut nalezena nerozpoznaná hodnota, správce front se nespustí, dokud nebude hodnota opravena.

IBM i Vlastnost **LogManagement** není v systému IBM iplatná.

Ruční (výchozí)
Oblasti protokolu spravujete ručně. Zadání této volby znamená, že správce front opakovaně nepoužívá ani neodstraňuje oblasti protokolu, a to ani v případě, že již nejsou zapotřebí pro obnovu.

Automatické
Oblasti protokolu jsou spravovány automaticky správcem front. Zadání této volby znamená, že správce front může opakovaně používat a odstraňovat oblasti protokolu, jakmile již nejsou zapotřebí pro obnovu. Nepřiděluje se žádná kapacita pro archivování.

Archiv
Oblasti protokolu jsou spravovány správcem front, ale po dokončení archivace jednotlivých oblastí protokolu je třeba upozornit správce front.

Zadání této volby znamená, že správce front může opakovaně používat a odstraňovat oblasti protokolu, jakmile mu je oznámeno, že určitá oblast, která již není zapotřebí pro obnovu, byla archivována.

Toto oznámení provedete pomocí příkazu **RESET QMGR** MQSC nebo pomocí příkazu Reset Queue Manager PCF.

Příklad stanza

```
Log:
   LogPrimaryFiles=3
   LogSecondaryFiles=2
   LogFilePages=4096
   LogType=CIRCULAR
   LogBufferPages=0
   LogPath=/var/mqm/log/saturn!queue!manager/
```

Poznámka: Hodnota nula pro **LogBufferPages** udává hodnotu 512.

Multi *LogWriteIntegrita-použití SingleWrite nebo TripleWrite*

Nastavení volby **LogWriteIntegrity** v sekci Protokol souboru `qm.ini` určuje algoritmus, který používá modul protokolování v produktu IBM MQ k zápisu záznamů protokolu do protokolu pro zotavení. Výchozí nastavení je `TripleWrite` a toto nastavení je bezpečné téměř ve všech možných scénářích.

Nastavení parametru **LogWriteIntegrity** má vůbec nějaký účinek, pouze když se má zapsat částečná stránka protokolu. Pro správce front s přiměřeným množstvím souběžné aktivity se tento scénář vyskytuje zřídka.

SingleWrite

`SingleWrite` vybere algoritmus, který může za velmi neobvyklých okolností fungovat lépe než výchozí nastavení `TripleWrite` . Nastavení `SingleWrite` je bezpečné pouze v případě, že základní platforma úložiště může za všech okolností zcela zaručit, že stránky 4KB zapsané synchronně do protokolu pro zotavení IBM MQ jsou zapsány atomicky.

Měli byste použít nastavení `SingleWrite` , pouze pokud systém souborů nebo zařízení hostující protokol obnovy IBM MQ výslovně zaručuje atomicitu 4KB zápisů. To znamená, že pokud dojde k selhání zápisu stránky 4KB z jakéhokoli důvodu, měly by být jediným možným stavem buď obraz před aktualizací, nebo obraz po spuštění, a že by neměl být možný žádný přechodný stav. Ve všech ostatních případech byste měli použít `TripleWrite`.

V systému s dostatečnou souběžností zapisuje správce front pouze celé stránky dat protokolu, a pokud je dosaženo vysokého procenta zaplnění stránek, není mezi parametry `SingleWrite` a `TripleWrite`významný rozdíl v výkonu.

V systému s malou souběžností může mít `SingleWrite`významnou výkonnostní výhodu, avšak upřednostňovaným řešením je obvykle zvýšení souběžnosti, spíše než použití `SingleWrite`.

Všimněte si, že může být obtížné spolehlivě určit atomicitu 4KB zápisů a změny základního softwaru nebo hardwaru mohou zneplatnit jakoukoli takovou záruku.

Máte-li jakékoli pochybnosti o tom, že vaše infrastruktura úložiště poskytuje požadované záruky nyní a kdykoli v budoucnosti za všech okolností, měli byste použít `TripleWrite`.

Windows LU62 sekce souboru qm.ini (pouzeWindows)

Sekce LU62 uvádí konfigurační parametry protokolu SNA LU 6.2 . Tyto parametry přepíší výchozí atributy pro kanály.

Použijte sekci LU62 v souboru `qm.ini` k uvedení konfiguračních parametrů protokolu SNA LU 6.2 . Přepíší výchozí atributy pro kanály.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer LU6.2 .

TPName
Název TP, který se má spustit na vzdáleném serveru.

Library1= *DLLName 1*
Název knihovny DLL APPC.

Výchozí hodnota je WCPIC32.

Library2= *DLLName2*
Totéž jako Library1, používá-li se kód uložený ve dvou samostatných knihovnách.

Výchozí hodnota je WCPIC32.

CP4I NativeHAInstance sekce souboru qm.ini

Pro IBM MQ v kontejnerech uvádí sekce `NativeHAInstance` , jak mohou tři uzly v konfiguraci nativní vysoké dostupnosti vzájemně komunikovat.

Poznámka: Tyto informace platí pouze pro kontejnerová prostředí. Viz téma Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operátor nebo Vytvoření skupiny nativní vysoké dostupnosti při vytváření vlastních kontejnerů.

Přidáte tři sekce `NativeHAInstance` , jednu pro každou instanci správce front v nativní skupině HA (včetně lokální instance). Přidejte následující atributy:

Název
Zadejte název instance, který jste použili při vytváření instance správce front.

ReplicationAddress
Uveďte název hostitele, adresu instance v hexadecimálním formátu IPv4 s tečkami nebo adresu instance v hexadecimálním formátu IPv6 . Adresu můžete uvést jako název hostitele, IPv4 tečkovou desítkovou adresu nebo IPv6 adresu v hexadecimálním formátu. Replikační adresa musí být rozpoznatelná a směrovatelná z každé instance ve skupině. Číslo portu, které se má použít pro replikaci protokolu, musí být uvedeno v závorkách, například:

```
ReplicationAddress=host1.example.com(4444)
```

Příklad stanza

Následující příklad ukazuje sekci `NativeHAInstance` použitou v souboru `qm.ini` k určení tří uzlů nativní konfigurace vysoké dostupnosti.

```
NativeHAInstance:
  Name=node-1
  ReplicationAddress=host1.example.com(4444)
NativeHAInstance:
  Name=node-2
  ReplicationAddress=host2.example.com(4444)
NativeHAInstance:
  Name=node-3
  ReplicationAddress=host3.example.com(4444)
```

Související pojmy

“NativeHALocalInstance sekce souboru qm.ini” na stránce 134
Pro IBM MQ v kontejnerech řídí sekce `NativeHALocalInstance` operaci nativní konfigurace vysoké dostupnosti.

CP4I NativeHALocalInstance sekce souboru qm.ini

Pro IBM MQ v kontejnerech řídí sekce `NativeHALocalInstance` operaci nativní konfigurace vysoké dostupnosti.

Poznámka: Tyto informace platí pouze pro kontejnerová prostředí. Viz téma Konfigurace nativní vysoké dostupnosti pomocí IBM MQ Operátor nebo Vytvoření skupiny nativní vysoké dostupnosti při vytváření vlastních kontejnerů.

Sekce `NativeHALocalInstance` se automaticky přidá do souboru `qm.ini` na každém z uzlů, když vytvoříte konfiguraci nativní vysoké dostupnosti. Pak můžete upravit soubor `qm.ini` a upravit atributy v sekci `NativeHALocalInstance` .

`LocalName`
Název sekce `NativeHALocalInstance` , převzatý z názvu instance repliky protokolu uvedeného při vytvoření správce front Nativní HA.

Do sekce `NativeHALocalInstance` můžete volitelně přidat následující atributy:

KeyRepository

V 9.3.0 V 9.3.0 Úplná cesta a název souboru úložiště klíčů, které obsahuje digitální certifikát používaný k ochraně provozu replikace protokolu. Pokud není uvedena přípona souboru, předpokládá se, že je `.kdb`.

Je-li atribut stanza `KeyRepository` vynechán, data replikace protokolu se vyměňují mezi instancemi v prostém textu.

V 9.3.2 **KeyRepositoryPassword**

Úložiště klíčů je zabezpečeno heslem, protože obsahuje citlivé informace. Chcete-li mít přístup k obsahu úložiště klíčů, produkt IBM MQ musí být schopen načíst heslo úložiště klíčů. Pokud heslo není uloženo v souboru pro dočasné ukládání úložiště klíčů, můžete je zadat do atributu `KeyRepositoryPassword` . Příklad:

```
KeyRepositoryPassword=passw0rd
```

Upozornění: Pokud zadáte heslo pomocí tohoto atributu, zašifrujte heslo pomocí systému ochrany hesla IBM MQ . Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 136.

V 9.3.2 **InitialKeyFile**

Tento atribut zadejte, pokud je heslo úložiště klíčů určené atributem `KeyRepositoryPassword` šifrováno pomocí specifického počátečního klíče. Název souboru, který obsahuje počáteční klíč, lze zadat pomocí parametru **-sf** , když se k zašifrování hesla úložiště klíčů použije příkaz **runmqicred** .

Nastavte hodnotu tohoto atributu na název souboru, který obsahuje počáteční klíč použitý k zašifrování hesla. Pokud například soubor s názvem `mykey.key` obsahuje počáteční klíč:

```
InitialKeyFile=/mykey.key
```

Další informace viz téma “Šifrování hesla úložiště klíčů” na stránce 136.

CertificateLabel

Popisek certifikátu identifikující digitální certifikát, který se má použít pro ochranu provozu replikace protokolu. Pokud je zadán parametr `KeyRepository` , ale parametr `CertificateLabel` je vynechán, použije se výchozí hodnota `ibmwebspheremq`*queue_manager* .

CipherSpec

CipherSpec , která má být použita k ochraně provozu replikace protokolu. Je-li uveden tento atribut stanza, musí být také uveden parametr `KeyRepository` . Pokud je zadán parametr `KeyRepository` , ale parametr `CipherSpec` je vynechán, použije se výchozí hodnota `ANY` .

LocalAddress

Adresa lokálního síťového rozhraní, která přijímá provoz replikace protokolu. Je-li uveden tento atribut stanza, identifikuje lokální síťové rozhraní a/nebo port ve formátu "[addr] [(port)]". Síťovou adresu lze zadat jako název hostitele, IPv4 tečkový desítkový formát nebo IPv6 hexadecimální formát. Pokud je tento atribut vynechán, správce front se pokusí svázat se všemi síťovými rozhraními, použije port uvedený v `ReplicationAddress` v sekci `NativeHAInstances` odpovídající názvu lokální instance.

HeartbeatInterval

Interval prezenčního signálu definuje, jak často, v milisekundách, aktivní instance správce front nativní vysoké dostupnosti odešle synchronizaci sítě. Platný rozsah hodnoty intervalu prezenčního signálu je 500 (0,5 s) do 60000 (1 min), hodnota mimo tento rozsah způsobí, že se správce front nespustí. Je-li tento atribut vynechán, použije se výchozí hodnota 5000 (5 s). Každá instance musí používat stejný interval prezenčního signálu.

HeartbeatTimeout

Časový limit prezenčního signálu definuje, jak dlouho bude instance repliky správce front nativní vysoké dostupnosti čekat, než se rozhodne, že aktivní instance nereaguje. Platný rozsah hodnoty časového limitu intervalu prezenčního signálu je 500 (0,5 s) do 120000 (2 min). Hodnota časového limitu prezenčního signálu musí být větší než nebo rovna intervalu prezenčního signálu.

Neplatná hodnota způsobí, že se správce front nespustí. Je-li tento atribut vynechán, čeká replika 2 x `HeartbeatInterval` před spuštěním procesu pro výběr nové aktivní instance. Každá instance musí používat stejný časový limit prezenčního signálu.

`RetryInterval`

Interval opakování definuje, jak často by se měl správce front nativní vysoké dostupnosti, v milisekundách, opakovat nezdařený odkaz na replikaci. Platný rozsah intervalu opakování je 500 (0,5 s) do 120000 (2 min). Je-li tento atribut vynechán, čeká replika 2 x `HeartbeatInterval` před zopakováním nezdařeného odkazu na replikaci.

`SSLFipsRequired`

Určuje, zda se používají pouze algoritmy certifikované podle standardu FIPS, pokud se šifrování používá při odesílání přenosů replikace protokolu. Nastavte na hodnotu `Yes` nebo `No`.

`EncryptionPolicySuiteB`

Určuje, zda provoz replikace protokolu používá šifrování vyhovující standardu Suite-B a jakou úroveň síly se používá. Nastavte jednu z následujících hodnot:

`NONE`
Šifrování vyhovující standardu Suite-B se nepoužívá. Toto nastavení je výchozí.

`128_BIT,192_BIT`
Nastaví sílu zabezpečení na 128bitovou i 192bitovou úroveň.

`128_BIT`
Nastaví sílu zabezpečení na 128bitovou úroveň.

`192_BIT`
Nastaví sílu zabezpečení na 192bitovou úroveň.

Šifrování hesla úložiště klíčů

V 9.3.2

Heslo úložiště klíčů lze chránit buď pomocí systému ochrany hesla IBM MQ , nebo pomocí souboru pro dočasné ukládání úložiště klíčů. Další informace o těchto dvou metodách naleznete v tématu Šifrování hesel úložiště klíčů.

Pokud je heslo úložiště uvedeno pomocí atributu `KeyRepositoryPassword` v sekci `NativeHALocalInstance` , zašifrujte heslo pomocí systému ochrany hesla IBM MQ . K zašifrování hesla použijte příkaz **`runmqicred`** . Příkaz vrátí šifrované heslo, které lze zadat v atributu `KeyRepositoryPassword` .

K bezpečnému zašifrování hesla použijte jedinečný počáteční klíč. Název souboru, který obsahuje počáteční klíč, lze zadat pomocí parametru **`-sf`** příkazu **`runmqicred`** . Pokud nezadáte jedinečný klíč, použije se výchozí klíč.

Pokud zašifrujete heslo úložiště klíčů pomocí jedinečného počátečního klíče, musíte také zadat stejný počáteční klíč pomocí atributu `InitialKeyFile` v sekci `NativeHALocalInstance` .

Příklad stanza

Následující příklad ukazuje sekci `NativeHALocalInstance` použitou v souboru `qm.ini` k uvedení lokálního názvu uzlu.

```
NativeHALocalInstance:
  LocalName=node-1
```

Související pojmy

“NativeHAInstance sekce souboru qm.ini” na stránce 134
Pro IBM MQ v kontejnerech uvádí sekce `NativeHAInstance` , jak mohou tři uzly v konfiguraci nativní vysoké dostupnosti vzájemně komunikovat.

Související odkazy

runmqicred (chránit hesla klienta IBM MQ)

Windows Sekce NETBIOS souboru qm.ini (pouzeWindows)

Sekce NETBIOS v souboru `qm.ini` uvádí konfigurační parametry protokolu NetBIOS . Tyto parametry přepíší výchozí atributy pro kanály.

Použijte sekci NETBIOS v souboru `qm.ini` , abyste uvedli konfigurační parametry protokolu NetBIOS . Přepíší výchozí atributy pro kanály.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer Netbios.

LocalName= *název*
Název, pod kterým je tento počítač známý v síti LAN.

AdapterNum = 0 (výchozí) | *adapter_number*
Číslo adaptéru LAN. Výchozí hodnota je adaptér 0.

NumSess = 1 (výchozí) | *počet_relací*
Počet relací, které se mají přidělit. Výchozí hodnota je 1.

NumCmds = 1 (výchozí) | *počet_příkazů*
Počet příkazů, které se mají přidělit. Výchozí hodnota je 1.

NumNames = 1 (výchozí) | *počet_názvů*
Počet názvů, které se mají přidělit. Výchozí hodnota je 1.

Library1= *DLLName1*
Název knihovny DLL NetBIOS .

Výchozí hodnota je NETAPI32.

Související pojmy

“Definování IBM MQ lokálního NetBIOS názvu” na stránce 255
Lokální název NetBIOS používaný procesy kanálu IBM MQ lze zadat třemi způsoby.

Linux AIX Sekce RestrictedMode souboru qm.ini

Sekce RestrictedMode určuje název skupiny obsahující členy, kteří mohou spouštět aplikace MQI, aktualizovat všechny prostředky IPCC a měnit obsah některých adresářů správce front. Tato sekce platí pouze pro systémy AIX and Linux .

Sekce RestrictedMode je nastavena volbou **-g** v příkazu **crtmqm** . Pokud nepoužijete volbu **-g** , sekce se nevytvoří v souboru `qm.ini` .

Existují adresáře, ve kterých aplikace IBM MQ vytvářejí soubory, zatímco jsou připojeny ke správci front v datovém adresáři správce front. Aby aplikace mohly vytvářet soubory v těchto adresářích, je jim udělen světový přístup pro zápis:

- `/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 uživatelé, kteří nepotřebují přístup ke správci front. Režim omezení upravuje oprávnění adresářů, které ukládají data správce front. K adresářům pak mohou přistupovat pouze členové uvedené skupiny aplikací. Stejným způsobem jsou také upravena oprávnění pro sdílenou paměť System V IPC používanou ke komunikaci se správcem front.

Skupina aplikací je název skupiny se členy, kteří mají oprávnění provádět následující akce:

- Spuštění aplikací MQI
- Aktualizovat všechny prostředky IPCC
- Změnit obsah některých adresářů správce front

Chcete-li pro správce front použít režim omezení, postupujte takto:

- Tvůrce správce front musí být ve skupině `mqm` a ve skupině aplikací.
- ID uživatele `mqm` musí být ve skupině aplikací.
- Všichni uživatelé, kteří chtějí spravovat správce front, musí být ve skupině `mqm` a ve skupině aplikací.
- Všichni uživatelé, kteří chtějí spustit aplikace IBM MQ , musí být ve skupině aplikací.

Všechna volání MQCONN nebo MQCONNX vydaná uživatelem, který není členem skupiny aplikací, se nezdaří s kódem příčiny MQRC_Q_MGR_NOT_AVAILABLE.

Důležité: Aby bylo možné rozeznat přidání uživatele do skupiny v mnoha operačních systémech, musí se příslušný uživatel odhlásit a znovu přihlásit.

Režim omezení pracuje se službou autorizace IBM MQ . Proto musíte také udělit uživatelům oprávnění pro připojení k produktu IBM MQ a přístup k prostředkům, které vyžadují, pomocí služby autorizace IBM MQ .

ALW Další informace o konfiguraci služby autorizace IBM MQ naleznete v části Nastavení zabezpečení na AIX, Linux, and Windows systémech.

Omezený režim IBM MQ používejte pouze v případě, že ovládací prvek poskytovaný autorizační službou neposkytuje dostatečnou izolaci prostředků správce front.

Související odkazy

`crtmqm` (vytvořit správce front)

Multi Sekce zabezpečení souboru qm.ini

Sekce Zabezpečení uvádí volby pro OAM (Object Authority Manager).

ClusterQueueAccessControl= RQMName | Xmitq

Tento atribut nastavte, chcete-li kontrolovat řízení přístupu k frontám klastru nebo k plně kvalifikovaným frontám, jejichž hostitelem jsou správci front klastru.

RQMNAME

Profily kontrolované pro řízení přístupu vzdáleně hostovaných front jsou pojmenované fronty nebo pojmenované profily správce front.

XMITQ

Profily kontrolované pro řízení přístupu vzdáleně hostovaných front jsou vyřešeny na `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

`Xmitq` je výchozí hodnota.

Windows **GroupModel=GlobalGroups**

Tento atribut určuje, zda modul OAM kontroluje globální skupiny při určování členství uživatele ve skupinách v systému Windows.

Výchozí nastavení je nekontrolovat globální skupiny.

GlobalGroups

OAM kontroluje globální skupiny.

V případě nastavení `GlobalGroups` příkazy autorizace **`setmqaut`**, **`dspmqaut`**a **`dmpmqaut`** přijímají globální názvy skupin; viz parametr **`setmqaut`** `-g` .

Poznámka: Nastavení parametru `ClusterQueueAcessControl=RQMName` a vlastní implementace služby autorizace na hodnotu nižší než `MQZAS_VERSION_6` způsobí, že se správce front nespustí.
V této instanci buď nastavte `ClusterQueueAcessControl=Xmitq` , nebo upgradujte vlastní autorizační službu na `MQZAS_VERSION_6` nebo vyšší.

Příklad stanza

```
Security:
      ClusterQueueAccessControl=Xmitq
      GroupModel=GlobalGroups
```

Multi Sekce služby souboru qm.ini

Sekce služby se používá k provedení změn instalovatelných služeb. Tato sekce obsahuje název služby a počet vstupních bodů definovaných pro službu.

Poznámka: Windows Linux Změna instalovatelných služeb a jejich komponent má významné důsledky. Z tohoto důvodu jsou instalovatelné služby v produktu IBM MQ Explorerjen pro čtení.

Pro každou komponentu v rámci služby musíte také zadat název a cestu k modulu obsahujícímu kód pro tuto komponentu. Pro tento účel použijte sekci ServiceComponent .

Sekce **Service** a **ServiceComponent** se mohou vyskytnout v libovolném pořadí a klíče sekce pod nimi se mohou také vyskytnout v libovolném pořadí. Pro každou z těchto sekcí musí být přítomny všechny klíče sekce. Je-li duplikován klíč sekce, použije se poslední.

Při spuštění správce front postupně zpracovává každou položku komponenty služby v konfiguračním souboru. Poté načte určený modul komponenty s vyvoláním vstupního bodu komponenty (který musí být vstupním bodem pro inicializaci komponenty) a předá mu popisovač konfigurace.

Název = AuthorizationService (výchozí) |NameService
Název požadované služby.

AuthorizationService
Pro systém IBM MQje komponenta **AuthorizationService** známá jako správce oprávnění k objektu nebo OAM. Sekce **Service** a přidružená sekce **ServiceComponent** jsou přidány automaticky při vytvoření správce front, ale lze je přepsat proměnnou prostředí *MQSNOAUT* . Přidejte další sekce **ServiceComponent** ručně.

Linux AIX Následující příklady sekcí v souboru `qm.ini` definují dvě komponenty služby autorizace na systému IBM MQ for AIX. *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

```
 Service:
    Name=AuthorizationService
    EntryPoints=13

 ServiceComponent:
    Service=AuthorizationService
    Name=MQSeries.UNIX.auth.service
Module=MQ_INSTALLATION_PATH/lib/amqzfu
    ComponentDataSize=0

 ServiceComponent:
    Service=AuthorizationService
    Name=user.defined.authorization.service
    Module=/usr/bin/udas01
    ComponentDataSize=96
```

Linux AIX Sekce ServiceComponent `MQSeries.UNIX.auth.service` definuje výchozí komponentu služby autorizace, OAM. Pokud odeberete tuto sekci a restartujete správce front, modul OAM bude zakázán a nebudou provedeny žádné kontroly autorizace.

Windows Můžete také přidat atribut **SecurityPolicy** pomocí služeb IBM MQ . Atribut **SecurityPolicy** se použije pouze v případě, že služba uvedená v sekci Služba je autorizační služba, tj. výchozí OAM. Atribut **SecurityPolicy** umožňuje určit zásadu zabezpečení pro každého správce front. Možné hodnoty jsou:

Výchozí
Chcete-li použít výchozí zásadu zabezpečení, zadejte hodnotu `Výchozí`. Pokud není identifikátor zabezpečení Windows (NT SID) OAM předán pro konkrétní ID uživatele, dojde k pokusu o získání příslušného identifikátoru SID vyhledáním v příslušných databázích zabezpečení.

NTSIDsRequired
Vyžaduje, aby byl identifikátor NT SID předán OAM při provádění kontrol zabezpečení.

Windows Sekce ServiceComponent `MQSeries.WindowsNT.auth.service` definuje výchozí komponentu služby autorizace, OAM. Pokud odeberete tuto sekci a restartujete správce front, modul OAM bude zakázán a nebudou provedeny žádné kontroly autorizace.

NameService
Standardně není poskytnuta žádná služba názvů. Pokud požadujete službu názvů, musíte přidat sekci NameService ručně.

Linux AIX Následující příklady sekcí souboru AIX and Linux `qm.ini` pro službu názvů uvádějí komponentu služby názvů poskytnutou (fiktivní) společností ABC.

```
# Stanza for name service
 Service:
    Name=NameService
    EntryPoints=5

# Stanza for name service component, provided by ABC
 ServiceComponent:
    Service=NameService
    Name=ABC.Name.Service
    Module=/usr/lib/abcname
    ComponentDataSize=1024
```

Poznámka: Windows Na systémech Windows jsou informace o sekci NameService uloženy v registru.

EntryPoints= *počet-položek*
Počet vstupních bodů definovaných pro službu.

To zahrnuje vstupní body inicializace a ukončení.

Windows **SecurityPolicy= Výchozí |NTSIDsRequired**
Na systémech Windows se atribut **`SecurityPolicy`** použije pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **`SecurityPolicy`** umožňuje určit zásadu zabezpečení pro každého správce front.

Možné hodnoty jsou:

Výchozí
Použijte výchozí zásadu zabezpečení, aby se projevila. Pokud není identifikátor zabezpečení Windows (NT SID) OAM předán pro konkrétní ID uživatele, dojde k pokusu o získání příslušného identifikátoru SID vyhledáním v příslušných databázích zabezpečení.

NTSIDsRequired
Při provádění kontrol zabezpečení předejte OAM identifikátor SID NT.

Další informace viz Windows identifikátory zabezpečení (SID).

Viz také Konfigurace sekcí autorizační služby: Windows systems.

Linux AIX **SecurityPolicy=user|group|UserExternal|default**
V systémech AIX and Linux hodnota uvádí, zda správce front používá autorizaci založenou na uživateli nebo na skupině. Hodnoty nerozlišují velikost písmen.

Hodnota může být jedna z následujících hodnot:

group = skupina
Správce front používá autorizaci založenou na skupině. Oprávnění pro přístup k prostředku je uděleno skupině.

Uživatel obdrží agregaci všech oprávnění, která jsou udělena každé skupině, do které patří.

ID uživatelů a skupiny musí být definovány pro lokální operační systém.

uživatel
Správce front používá autorizaci založenou na uživateli. Oprávnění pro přístup k prostředku lze udělit skupině nebo určitému ID uživatele.

Uživatel obdrží agregaci následujících oprávnění:

- Oprávnění, která jsou udělena konkrétnímu uživateli.
- Oprávnění, která jsou udělena každé skupině, do které uživatel patří.

ID uživatelů a skupiny musí být definovány pro lokální operační systém.

V 9.3.0 **UserExternal**
Správce front používá autorizaci založenou na uživateli. Oprávnění však mohou být udělena ID uživatelů, která nejsou známa lokálnímu operačnímu systému.

Oprávnění pro přístup k prostředku lze udělit skupině nebo určitému ID uživatele.

Uživatel obdrží agregaci následujících oprávnění:

- Oprávnění, která jsou udělena konkrétnímu uživateli.
- Oprávnění, která jsou udělena každé skupině, do které uživatel patří.

Pokud lokální operační systém uživatele nezná, je považován za uživatele, který patří pouze do skupiny nikdo. Další informace o skupinách naleznete v tématu Činitele a skupiny na webu AIX, Linux, and Windows. ID uživatele musí být dlouhé až 12 znaků a musí odpovídat pravidlům pro pojmenovávání IBM MQ objektů.

Můžete upravit existující správce front tak, aby používal tuto další volbu bez ztráty aktuální konfigurace.

V 9.3.4 Toto je výchozí hodnota, pokud je uvedena sekce AuthToken .

default
Správce front používá autorizaci založenou na skupině. Chování je stejné jako u volby `group` .

Toto je výchozí hodnota, pokud není uvedena sekce AuthToken .

Restartujte správce front, aby se změny hodnoty atributu projevily.

Poznámka: Linux V 9.3.4 AIX Pokud je v produktu IBM MQ 9.3.4uvedena sekce AuthToken , efektivní hodnota atributu **SecurityPolicy** sekce Service je nastavena na `UserExternal`. Ověření tokenu není k dispozici, pokud je **SecurityPolicy** explicitně nastaveno na `Skupina` v sekci Služba. Je-li parametr **SecurityPolicy** nastaven na hodnotu `Skupina`, odeberte atribut **SecurityPolicy** ze sekce služby a poté restartujte správce front. Další informace viz “Sekce AuthToken souboru qm.ini” na stránce 111.

SharedBindingsUserId= ***typ uživatele***
Atribut **SharedBindingsUserId** platí pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **SharedBindingsUserId** se používá pouze ve vztahu ke sdíleným vazbám. Tato hodnota vám umožňuje určit, zda pole *UserIdentifier* ve struktuře *IdentityContext* z funkce MQZ_AUTHENTICATE_USER je efektivní ID uživatele nebo skutečné ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu MQZ_AUTHENTICATE_USER-Ověření uživatele.

Možné hodnoty jsou:

Výchozí
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** platí pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **FastpathBindingsUserId** se používá pouze ve vztahu k vazbám rychlé cesty. Tato hodnota vám umožňuje určit, zda pole *UserIdentifier* ve struktuře *IdentityContext* z funkce MQZ_AUTHENTICATE_USER je efektivní ID uživatele nebo skutečné ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu MQZ_AUTHENTICATE_USER-Ověření uživatele.

Možné hodnoty jsou:

Výchozí
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** platí pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **IsolatedBindingsUserId** se používá pouze s relací k izolovaným vazbám. Tato hodnota vám umožňuje určit, zda pole *UserIdentifier* ve struktuře *IdentityContext* z funkce MQZ_AUTHENTICATE_USER je efektivní ID uživatele nebo skutečné ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu MQZ_AUTHENTICATE_USER-Ověření uživatele.

Možné hodnoty jsou:

Výchozí
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 naleznete v tématu Instalovatelné služby a komponenty pro produkt AIX, Linux, and Windows.

Další informace o službách zabezpečení obecně naleznete v tématu Nastavení zabezpečení na systémech AIX and Linux.

Příklad stanza

```
Service:
   Name=AuthorizationService
   EntryPoints=14
```

Související pojmy
Instalovatelné služby a komponenty pro systémy AIX, Linuxa Windows
Související odkazy
Instalovatelné služby a komponenty na systému IBM i
Referenční informace o instalovatelných službách

Multi Sekce ServiceComponent souboru qm.ini

Sekce ServiceComponent uvádí informace pro komponentu služby. Při přidávání nové instalovatelné služby musíte zadat informace o komponentě služby. Standardně je přítomna sekce autorizační služby a přidružená komponenta, OAM, je aktivní.

Sekce **Service** a **ServiceComponent** se mohou vyskytnout v libovolném pořadí a klíče sekce pod nimi se také mohou vyskytnout v libovolném pořadí. Pro každou z těchto sekcí musí být přítomny všechny klíče sekce. Je-li duplikován klíč sekce, použije se poslední.

Při spuštění správce front postupně zpracovává každou položku komponenty služby v konfiguračním souboru. Poté načte určený modul komponenty s vyvoláním vstupního bodu komponenty (který musí být vstupním bodem pro inicializaci komponenty) a předá mu popisovač konfigurace.

Služba = *název_služby*
Název požadované služby. Musí se shodovat s hodnotou uvedenou v atributu Name informací o konfiguraci služby.

Název = *název_komponenty*
Popisný název komponenty služby. Musí být jedinečný a obsahovat pouze znaky, které jsou platné pro názvy objektů IBM MQ (například názvy front). Tento název se vyskytuje ve zprávách operátora generovaných službou. Doporučujeme, aby tento název začínával ochrannou známkou společnosti nebo podobným rozlišovacím řetězcem.

Module = *název_modulu*
Název modulu, který má obsahovat kód pro tuto komponentu. Musí se jednat o úplný název cesty.

ComponentDataVelikost = *velikost*
Velikost datové oblasti komponenty předané komponentě při každém volání v bajtech. Pokud nejsou vyžadována žádná data komponenty, zadejte hodnotu nula.

Příklad stanza

```
ServiceComponent:
   Service=AuthorizationService
   Name=MQSeries.UNIX.auth.service
   Module=amqzfu
   ComponentDataSize=0
```

Další příklady zobrazující sekci AuthorizationService a přidružené sekce ServiceComponent a sekci NameService a přidruženou sekci ServiceComponent viz “Sekce služby souboru qm.ini” na stránce 139.

Související pojmy
Instalovatelné služby a komponenty pro systémy AIX, Linuxa Windows
Související odkazy
“Sekce služby souboru qm.ini” na stránce 139
Sekce služby se používá k provedení změn instalovatelných služeb. Tato sekce obsahuje název služby a počet vstupních bodů definovaných pro službu.
Instalovatelné služby a komponenty na systému IBM i
Referenční informace o instalovatelných službách

Windows Sekce SPX souboru qm.ini (pouzeWindows)

Sekce SPX uvádí konfigurační parametry protokolu SPX. Tyto parametry přepíší výchozí atributy pro kanály.

Pomocí sekce SPX v souboru `qm.ini` zadejte konfigurační parametry protokolu SPX.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer SPX .

Soket = 5E86 (výchozí) | *číslo_soketu*
Číslo soketu SPX v hexadecimální notaci. Výchozí hodnota je X'5E86'.

BoardNum = 0 (výchozí) | *číslo_adaptéru*
Číslo adaptéru LAN. Výchozí hodnota je adaptér 0.

KeepAlive= NE | ANO
Zapněte nebo vypněte funkci KeepAlive .

KeepAlive=YES způsobuje, že SPX pravidelně kontroluje, zda je druhý konec připojení stále k dispozici. Pokud není, kanál se zavře.

Library1= *DLLName1*
Název knihovny DLL SPX.

Výchozí hodnota je WSOCK32.DLL.

Library2= *DLLName2*
Stejné jako LibraryName1, používá se, pokud je kód uložen ve dvou samostatných knihovnách.

Výchozí hodnota je WSOCK32.DLL.

ListenerBacklog= číslo
Přepsat výchozí počet nevyřízených požadavků pro modul listener SPX.

Při příjmu na SPX je nastaven maximální počet nevyřízených požadavků na připojení. Toto může být považováno za nevyřízené požadavky čekající na soket SPX, aby listener přijal požadavek. Výchozí hodnoty seznamu nevyřízených požadavků modulu listener jsou uvedeny v souboru Tabulka 13 na stránce 144.

Tabulka 13. Výchozí nevyřízené požadavky na připojení (SPX)

Platforma	**Výchozí hodnota ListenerBacklog**
Server Windows	100
Windows Pracovní stanice	5

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí hodnota. Použijte tuto volbu, abyste se vyhnuli dosažení limitu připojení.

Naopak, některé operační systémy mohou omezit velikost nevyřízených požadavků SPX, takže efektivní nevyřízené požadavky SPX mohou být menší, než je požadováno zde.

Pokud nevyřízené požadavky dosáhnou hodnot zobrazených v souboru Tabulka 13 na stránce 144, připojení SPX je odmítnuto a kanál nelze spustit. V případě kanálů zpráv to vede k tomu, že kanál přejde do stavu OPAKOVAT a později se znovu pokusí o připojení. V případě připojení klienta obdrží klient kód příčiny MQRC_Q_MGR_NOT_AVAILABLE z MQCONN a měl by připojení zopakovat později.

Multi Sekce SSL souboru qm.ini

Sekce SSL se používá ke konfiguraci kanálů 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 kanálům SSL nebo TLS ve správci front používat rozšíření přístupu AuthorityInfoAccess, ujistěte se, že server OCSP, který je v nich uveden, je dostupný, je správně nakonfigurován a je přístupný po síti. Další informace naleznete v tématu Práce se zrušenými certifikáty.

CrlDistributionBod (CDP)

Certifikát může obsahovat rozšíření bodu CrlDistribution. Toto rozšíření obsahuje adresu URL, která identifikuje jak protokol použitý ke stažení seznamu odvolaných certifikátů (CRL), tak i server, který má být kontaktován.

Chcete-li povolit kanálům SSL nebo TLS ve správci front používat rozšíření bodu CrlDistribution, ujistěte se, že server CDP, který je v nich uveden, je dostupný, správně nakonfigurovaný a přístupný v síti.

Stanza zabezpečení SSL

Pomocí sekce SSL v souboru `qm.ini` nakonfigurujte, jak se kanály TLS ve vašem správci front pokusí použít následující prostředky a jak budou reagovat v případě, že při jejich použití dojde k problémům.

Pokud v každém z následujících případů zadaná hodnota není jednou z platných hodnot uvedených v seznamu, použije se výchozí hodnota. Nejsou zapsány žádné chybové zprávy uvádějící, že byla zadána neplatná hodnota.

V 9.3.0 **OutboundSNI = CHANNEL | HOSTNAME**

Je-li parametr **OutboundSNI** nastaven na hodnotu CHANNEL, klienti s podporou SNI nastaví při inicializaci připojení TLS název cílového kanálu IBM MQ na vzdálený systém.

Je-li tento atribut nastaven na hodnotu HOSTNAME, klienti s podporou SNI nastaví záhlaví SNI na název hostitele, což způsobí, že požadavky na odchozí připojení obdrží výchozí certifikát vzdáleného správce front během navázání komunikace TLS, a proto nelze použít certifikáty pro jednotlivé kanály.

Poznámka: Pokud se **OutboundSNI**=HOSTNAME používá pro připojení ke vzdálenému kanálu s nakonfigurovaným popiskem certifikátu, připojení se odmítne s MQRC_SSL_INITIALIZATION_ERROR a do protokolů chyb vzdáleného správce front se vytiskne zpráva AMQ9673 .

AllowOutboundSNI = YES (výchozí) | NE

Je-li tato volba povolena, klienti s podporou SNI nastaví SNI na název cílového kanálu IBM MQ pro vzdálený systém při inicializaci připojení TLS. Je-li tento atribut nastaven na hodnotu NO, klienti s podporou SNI nenastaví záhlaví SNI, což způsobí, že požadavky na odchozí připojení obdrží výchozí certifikát vzdáleného správce front během navázání komunikace TLS, a proto nelze použít certifikáty pro jednotlivé kanály.

Upozornění: Deprecated V 9.3.0 From IBM MQ 9.3.0 the **AllowOutboundSNI** property is deprecated, and is available for backwards-compatibility purposes only.

AllowOutboundSNI set to YES poskytuje stejnou funkci jako **OutboundSNI** nastavenou na CHANNEL, zatímco **AllowOutboundSNI** nastavenou na NO poskytuje stejnou funkci jako **OutboundSNI** nastavenou na HOSTNAME.

Pokud jsou v sekci SSL přítomny atributy **AllowOutboundSNI** i **OutboundSNI** , má přednost nastavení **OutboundSNI** .

AllowedCipherSpecifikace =*název|seznam názvů*| ALL

Určuje vlastní seznam CipherSpecs , které jsou seřazeny a povoleny pro použití s kanály IBM MQ na platformě Multiplatforms.

- Jeden název CipherSpec .
- Čárkami oddělený seznam názvů IBM MQ CipherSpec , které chcete znovu povolit.
- Speciální hodnota ALLpředstavující všechny CipherSpecs (nedoporučuje se).

Poznámka: Neměli byste vybrat volbu **ALL** CipherSpecs, protože to umožňuje protokoly SSL 3.0 a TLS 1.0 a velký počet slabých šifrovacích algoritmů.

Další informace naleznete v tématu Poskytnutí vlastního seznamu seřazených a povolených CipherSpecs v systému IBM MQ for Multiplatforms v pořadí CipherSpec v navázání komunikace TLS.

IBM i ALW **AllowTLSV13 =Y | YES | T | TRUE (výchozí) | N | NO | F | FALSE**

Určuje, zda může správce front používat specifikaci TLS 1.3 CipherSpecs.

- Y (výchozí), YES (výchozí), T (výchozí) nebo TRUE (výchozí): Povoluje protokol TLS 1.3 , který umožňuje správci front používat protokol TLS 1.3 CipherSpecs.
- N, NO, Fnebo FALSE: Zakáže protokol TLS 1.3, což znamená, že správce front nemůže používat protokol TLS 1.3 CipherSpecs.

Další informace naleznete v tématu Povolení CipherSpecs.

CDPCheckExtensions= YES |NO (výchozí)

Určuje, zda se kanály TLS v tomto správci front pokusí zkontrolovat servery CDP pojmenované v rozšířeních certifikátu CrlDistributionPoint.

- YES: Kanály TLS se pokusí zkontrolovat servery CDP a určit, zda je digitální certifikát odvolán.
- NO (výchozí): Kanály TLS se nepokoušejí kontrolovat servery CDP. Tato hodnota je výchozí.

ALW **MinimumRSAKeyvelikost=int**

Určuje minimální velikost klíče, kterou musí mít certifikáty RSA, aby mohly být přijaty během navázání komunikace TLS. Povoluje jakoukoli hodnotu rovnající se 0 nebo vyšší. Není-li uvedeno, použije se výchozí hodnota 1.

OCSPAuthentication=REQUIRED (výchozí) | WARN | OPTIONAL

Určuje akci, která má být provedena v případě, že ze serveru OCSP nelze určit stav odvolání.

Je-li povolena kontrola OCSP, program kanálu TLS se pokusí kontaktovat server OCSP.

Pokud program kanálu nemůže kontaktovat žádné servery OCSP nebo pokud žádný server nemůže poskytnout stav odvolání certifikátu, použije se hodnota parametru OCSPAuthentication.

- REQUIRED (výchozí nastavení): Selhání při určení stavu odvolání způsobí zavření připojení s chybou. Tato hodnota je výchozí.
- VAROVÁNÍ: Selhání při zjišťování stavu odvolání způsobí, že se do protokolu chyb správce front zapíše varovná zpráva, ale připojení může pokračovat.
- VOLITELNÉ: Selhání při zjišťování stavu odvolání umožňuje připojení pokračovat v bezobslužném režimu. Nejsou uvedena žádná varování nebo chyby.

OCSPCheckExtensions = YES (výchozí) | NE

Určuje, zda se kanály TLS v tomto správci front pokusí zkontrolovat servery OCSP, které jsou pojmenovány v rozšířeních přístupového certifikátu AuthorityInfo.

- YES (výchozí nastavení): Kanály TLS se pokusí zkontrolovat servery OCSP a určit, zda je digitální certifikát odvolán. Tato hodnota je výchozí.
- NO: Kanály TLS se nepokoušejí kontrolovat servery OCSP.

ALW **OCSPTimeout= *number***

Počet sekund čekání na odpovídací modul OCSP při provádění kontroly odvolání.

Pokud je v systému IBM MQ 9.3.0nastavena hodnota 0, použije se výchozí časový limit 30 sekund.

Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 30 sekund.

SSLHTTPProxyName= *řetězec*

Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má produkt IBM Global Security Kit (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.

AIX Pro 32bitové klienty v systému AIXmůže být síťová adresa pouze adresou IPv4 .

Na jiných platformách může být síťová adresa IPv4 nebo IPv6 .

Tento atribut může být nezbytný například v případě, že brána firewall zabraňuje přístupu k adrese URL odpovídacího modulu OCSP.

ALW **PeerCertChainValidation=*řetězec***

Řetězec může mít jednu ze dvou hodnot:

- `Usepeerchain` **[výchozí]**: Řetěz certifikátů poskytnutý rovnocenným partnerem lze použít k překlenutí případných mezer v řetězu důvěryhodnosti při ověřování certifikátů. S výjimkou kořenového certifikátu.
- `Pouze úložiště údajů o důvěryhodnosti` **[Nedoporučeno]**: Pro ověření certifikátu partnera budou použity pouze certifikáty v úložišti údajů o důvěryhodnosti.

ALW **SSLHTTPConnectTimeout= *číslo*|0**

Počet sekund čekání na úspěšné vytvoření síťového připojení k serveru HTTP při provádění kontroly odvolání.

Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 0 (vypnuto).

Příklad stanza

```
SSL:
       OutboundSNI=CHANNEL
       AllowedCipherSpecs=TLS13 CipherSpec list
       AllowTLSV13=Y
       CDPCheckExtensions=NO
       MinimumRSAKeySize=1
       OCSPAuthentication=REQUIRED
       OCSPCheckExtensions=YES
       OCSPTimeout=30
       PeerCertChainValidation=Usepeerchain
       SSLHTTPConnectTimeout=0
```

Notes:

- Výchozí hodnota parametru **`OutboundSNI`** je **`Channel`**.
- Seznam **`TLS13 CipherSpec`** je seznam specifických CipherSpecs , nikoli šifry aliasů. Pokud požadujete pouze šifry TLS1.3 , musíte je vypsat. Příklad:

  TLS_CHACHA20_POLY1305_SHA256
  TLS_AES_256_GCM_SHA384
  TLS_AES_128_GCM_SHA256
  TLS_AES_128_CCM_SHA256
  TLS_AES_128_CCM_8_SHA256
- Výchozí hodnota parametru **`AllowTLSV13`** je Y , pokud jste nepovolili slabé šifry. V takovém případě se tato volba vypne (pokud ji explicitně nezapnete).
- Hodnoty parametru **`CDPCheckExtensions`** mohou být pouze Ano nebo Ne.
- Hodnoty parametru **`PeerCertChainValidation`** mohou být pouze `Usepeerchain` nebo `Truststoreonly`.

Multi Sekce podfondu souboru qm.ini

Tuto sekci vytváří IBM MQ. Neměňte ji.

Sekci Dílčí fond a atribut **`ShortSubpoolName`** v rámci této sekce zapisuje produkt IBM MQ automaticky při vytváření správce front. IBM MQ zvolí hodnotu pro **`ShortSubpoolName`**. Tuto hodnotu neměňte.

Název odpovídá adresáři a symbolickému odkazu vytvořenému v adresáři `/var/mqm/sockets` , který produkt IBM MQ používá pro interní komunikaci mezi běžícími procesy.

Multi Sekce TCP souboru qm.ini

Sekce TCP uvádí konfigurační parametry TCP/IP (Transmission Control Protocol/Internet Protocol). Tyto parametry přepíší výchozí atributy pro kanály.

Použijte sekci TCP v souboru `qm.ini` , abyste uvedli konfigurační parametry TCP/IP.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front IBM MQ Explorer SPX TCP.

Port = 1414 (výchozí) | *číslo_portu*
Výchozí číslo portu v desítkové notaci pro relace TCP/IP. *Dobře známé* číslo portu pro IBM MQ je 1414.

Windows **Library1= *DLLName1* (pouzeWindows)**
Název knihovny DLL soketů TCP/IP.

Výchozí hodnota je WSOCK32.

Multi V 9.3.0 **SecureCommsOnly = NO | N | FALSE | F (výchozí) |TRUE | T | YES | Y**
Určete, zda je povolena komunikace v prostém textu.

SecureCommsOnly=NO | N | FALSE | F
Komunikace v prostém textu je povolena a při spuštění správce front se zobrazí varovná zpráva.

SecureCommsOnly=YES | Y | TRUE | T
Komunikace v prostém textu není povolena a při spuštění správce front je zobrazena informační zpráva.

KeepAlive = NO (výchozí) |ANO
Zapněte nebo vypněte funkci KeepAlive . KeepAlive=YES způsobuje, že TCP/IP pravidelně kontroluje, zda je druhý konec připojení stále k dispozici. Pokud není, kanál se zavře.

ListenerBacklog= číslo
Přepsat výchozí počet neprovedených požadavků pro modul listener TCP/IP.

Při příjmu v protokolu TCP/IP je nastaven maximální počet nevyřízených požadavků na připojení. To lze považovat za nevyřízené požadavky požadavků čekajících na port TCP/IP, aby mohl modul listener přijmout požadavek. Výchozí hodnoty seznamu nevyřízených požadavků modulu listener jsou zobrazeny v souboru Tabulka 14 na stránce 148.

Tabulka 14. Výchozí nevyřízené požadavky na připojení (TCP)

Platforma	Výchozí hodnota ListenerBacklog
Windows Windows Server	100
Linux Linux	100
AIX AIX V5.3 nebo novější	100

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí hodnota. Použijte tuto volbu, abyste se vyhnuli dosažení limitu připojení.

Naopak, některé operační systémy mohou omezit velikost nevyřízených požadavků TCP, takže efektivní nevyřízené požadavky TCP mohou být menší, než je zde požadováno.

Pokud nevyřízené požadavky dosáhnou hodnot uvedených v části Tabulka 14 na stránce 148, připojení TCP/IP je odmítnuto a kanál nelze spustit. V případě kanálů zpráv to vede k tomu, že kanál přejde do stavu OPAKOVAT a později se znovu pokusí o připojení. V případě připojení klienta obdrží klient kód příčiny MQRC_Q_MGR_NOT_AVAILABLE od `MQCONN` a pokusí se o připojení později.

Následující skupinu vlastností lze použít k řízení velikosti vyrovnávacích pamětí používaných protokolem TCP/IP. Hodnoty se předávají přímo do vrstvy TCP/IP operačního systému. Při používání těchto vlastností

je třeba věnovat velkou pozornost. Pokud jsou hodnoty nastaveny nesprávně, může to nepříznivě ovlivnit výkon TCP/IP. Další informace o tom, jak to ovlivňuje výkon, naleznete v dokumentaci TCP/IP pro vaše prostředí. Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávacích pamětí, na rozdíl od velikostí vyrovnávacích pamětí, které jsou opraveny produktem IBM MQ.

Časový limit připojení = 0 (výchozí) |číslo
Počet sekund do vypršení časového limitu pokusu o připojení soketu. Výchozí hodnota nula určuje, že neexistuje žádný časový limit připojení.

Procesy kanálu IBM MQ se připojují přes neblokující sokety. Pokud tedy druhý konec soketu není připraven, funkce connect () se okamžitě vrátí s volbou *EINPROGRESS* nebo *EWOULDBLOCK*. Po tomto pokusu dojde k pokusu o připojení, a to až do celkového počtu 20 takových pokusů, když je ohlášena chyba komunikace.

Je-li volba `Časový limit připojení` nastavena na nenulovou hodnotu, produkt IBM MQ čeká po stanovenou dobu na volání select (), aby se soket dostal do stavu Připraven. Tím se zvýší šance na úspěch následného volání connect (). Tato volba může být užitečná v situacích, kdy by připojení vyžadovala určitou čekací dobu kvůli vysokému zatížení sítě.

SndBuffSize = číslo |0 (výchozí)
Velikost vyrovnávací paměti pro odesílání TCP/IP použité odesílajícím koncem kanálů v bajtech. Tuto hodnotu sekce lze přepsat stanzou specifičtější pro typ kanálu, například RcvSndBuffSize. Je-li hodnota nastavena na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

Multi V produktu IBM MQ 8.0jsou automaticky vytvářeni noví správci front s výchozím nastavením 0 (viz “Příklad stanza” na stránce 150.

RcvBuffSize = číslo |0 (výchozí)
Velikost vyrovnávací paměti pro příjem TCP/IP použité přijímacím koncem kanálů v bajtech. Tuto hodnotu sekce lze přepsat stanzou specifičtější pro typ kanálu, například RcvRcvBuffSize. Je-li hodnota nastavena na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

Multi V produktu IBM MQ 8.0jsou automaticky vytvářeni noví správci front s výchozím nastavením 0 (viz “Příklad stanza” na stránce 150.

RcvSndBuffSize = číslo |0 (výchozí)
Velikost vyrovnávací paměti pro odesílání protokolu TCP/IP používané koncem odesilatele přijímacího kanálu v bajtech. Je-li hodnota nastavena na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

Multi V produktu IBM MQ 8.0jsou automaticky vytvářeni noví správci front s výchozím nastavením 0 (viz “Příklad stanza” na stránce 150.

RcvRcvBuffSize = číslo |0 (výchozí)
Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech, kterou používá přijímající strana přijímacího kanálu. Je-li hodnota nastavena na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

Multi V produktu IBM MQ 8.0jsou automaticky vytvářeni noví správci front s výchozím nastavením 0 (viz “Příklad stanza” na stránce 150.

SvrSndBuffSize = číslo |0 (výchozí)
Velikost vyrovnávací paměti pro odesílání TCP/IP v bajtech, kterou používá server na konci kanálu připojení serveru připojení klienta. Je-li hodnota nastavena na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

Multi V produktu IBM MQ 8.0jsou automaticky vytvářeni noví správci front s výchozím nastavením 0 (viz “Příklad stanza” na stránce 150.

SvrRcvBuffSize = číslo |0 (výchozí)
Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech, kterou používá konec serveru kanálu připojení serveru připojení klienta. Je-li hodnota nastavena na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

Multi V produktu IBM MQ 8.0jsou automaticky vytvářeni noví správci front s výchozím nastavením 0 (viz “Příklad stanza” na stránce 150).

Příklad stanza

```
TCP:
  SndBuffSize=0
  RcvBuffSize=0
  RcvSndBuffSize=0
  RcvRcvBuffSize=0
  ClntSndBuffSize=0
  ClntRcvBuffSize=0
  SvrSndBuffSize=0
  SvrRcvBuffSize=0
```

Poznámka: Multi Pro nové správce front v systému Multiplatforms je výchozí velikost vyrovnávací paměti pro odesílání a příjem protokolu TCP v sekci TCP konzoly `qm.ini file` nastavena tak, aby byla spravována operačním systémem. Jak je uvedeno v předchozím příkladu, noví správci front jsou automaticky vytvořeni s výchozím nastavením 0 pro vyrovnávací paměti pro odesílání a příjem. Toto platí pouze pro nové správce front. Nastavení vyrovnávací paměti pro odesílání a příjem protokolu TCP pro správce front, kteří jsou migrováni ze starších verzí produktu IBM MQ , jsou zachována.

Pokud jsou ze souboru `qm.ini` odebrány vlastnosti velikosti vyrovnávací paměti TCP, je výchozí vyrovnávací paměť nastavena na hodnotu 32K. Při použití tohoto výchozího nastavení byste měli postupovat opatrně, protože 32K nemusí být vhodnou vyrovnávací pamětí pro všechny scénáře systému zpráv.

Pokud jsou vlastnosti vyrovnávací paměti pro odesílání a příjem TCP nastaveny na nulu, použijí se výchozí hodnoty OS. Metoda výběru těchto předvoleb se bude lišit podle operačního systému, ale obvykle se nachází v manuálových stránkách "tcp" nebo get/setsockopt () OS.

Multi `TuningParameters` sekce souboru qm.ini

Sekce TuningParameters určuje volby pro vyladění správce front.

SuppressDspAuthFail= YES |NO (výchozí)
Je-li nastavena hodnota YES, správce front potlačí generování událostí autorizace a zápis chybových zpráv AMQ8077 do protokolu chyb při selhání kontroly autorizace, pokud připojení nemá k objektu oprávnění + dsp.

ImplSyncOpenOutput=*hodnota*
`ImplSyncOpenOutput` je minimální počet aplikací, které mají otevřenou frontu pro vložení, než bude možné povolit implicitní synchronizační bod pro trvalé vložení mimo synchronizační bod. Výchozí hodnota **`ImplSyncOpenOutput`** je 2.

To má za následek, že pokud existuje pouze jedna aplikace, která má tuto frontu otevřenou pro operaci vložení, **`ImplSyncOpenOutput`** se vypne.

Zadání parametru `ImplSyncOpenOutput=1` znamená, že bude vždy brán v úvahu implicitní synchronizační bod. Můžete nastavit libovolnou kladnou celočíselnou hodnotu. Pokud nikdy nechcete přidat implicitní synchronizační bod, nastavte `ImplSyncOpenOutput=OFF`.

UniformClusterNázev =*název klastru*
Název klastru IBM MQ , který používáte jako jednotný klastr.

OAMLdapConnectTimeout=čas|0 (výchozí)
Maximální doba v sekundách, po kterou bude klient LDAP čekat na vytvoření připojení TCP k serveru. Pokud prostřednictvím seznamu názvů připojení zadáváte více serverů LDAP, bude časový limit platit

pro každý jednotlivý pokus o připojení, a proto dojde při dosažení tohoto časového limitu k pokusu o připojení k další položce v seznamu názvů.

čas má maximální hodnotu 3600 sekund a hodnota 0, což je minimální hodnota, stejně jako výchozí hodnota, znamená, že čekání je neomezené.

OAMLdapQueryTimeLimit=čas|0 (výchozí)
Maximální doba (v sekundách), po kterou bude klient LDAP čekat na přijetí odpovědi na požadavek LDAP ze serveru, po navázání připojení a odeslání požadavku LDAP.

čas má maximální hodnotu 3600 sekund a hodnota 0, což je minimální hodnota, stejně jako výchozí hodnota, znamená, že čekání je neomezené.

V 9.3.0.5 V 9.3.2 **OAMLdapResponseWarningTime=*prahová hodnota***
Pokud připojení k serveru LDAP trvalo déle, než je prahová hodnota v sekundách určená parametrem **OAMLdapResponseWarningTime** , bude do protokolu chyb zapsána zpráva AMQ5544W . Výchozí prahová hodnota je 10 sekund.

ExpiryInterval
Označuje frekvenci, s jakou správce front prochází fronty a hledá zprávy s vypršenou platností, které dosud nebyly vyčištěny jinými aktivitami fronty. Jedná se o časový interval v sekundách.

Standardně se skener vypršení spouští přibližně každých pět minut na produkčních IBM MQ sestaveních.

POZOR: Změna hodnoty **ExpiryInterval** není obvykle vyžadována a tuto hodnotu byste měli upravit pouze pod vedením podpory IBM .

LivenessHeartBeatLen
Konfiguruje četnost provádění kontrol správce front, který zapisuje do protokolu, v rozumné míře. Maximální hodnota pro **LivenessHeartBeatLen** je 600 sekund (10 minut) a minimální hodnota je 0, což má za následek vypnutí kontroly úplně.

POZOR: Ve většině případů není nutné měnit četnost těchto kontrol. Neprovádět žádné změny, pokud vám to nedoporučí podpora IBM .

ECHeartBeatcs
Konfiguruje frekvenci obecných kontrol stavu správce front. Minimální hodnota pro **ECHeartBeatLen** je 10000 milisekund (10 sekund) a maximální hodnota je 60000 milisekund (60 sekund).

POZOR: Ve většině případů není nutné měnit četnost těchto kontrol. Neprovádět žádné změny, pokud vám to nedoporučí podpora IBM .

FileLockHeartBeatdélka
Změní výchozí hodnotu pro kontrolu zámků souborů pro správce front s více instancemi, kterou řadič provedení pravidelně provádí, aby se ujistil, že stále drží výlučný zámek na primárním souboru s více instancemi. Standardně se tyto kontroly zámků souborů provádějí každých 20 sekund. Minimální hodnota pro **FileLockHeartBeatLen** je 10 sekund a maximální hodnota je 600 sekund (10 minut).

POZOR: Ve většině případů není nutné měnit četnost těchto kontrol. Neprovádět žádné změny, pokud vám to nedoporučí podpora IBM .

Příklad stanza

V 9.3.0.5 V 9.3.2

```
TuningParameters:
       SuppressDspAuthFail=NO
       ImplSyncOpenOutput=2
       OAMLdapConnectTimeout=60
       OAMLdapQueryTimeLimit=60
       OAMLdapResponseWarningTime=10
       ExpiryInterval=300
```

Související pojmy

Implicitní synchronizační bod

Multi Sekce proměnných souboru qm.ini

Sekce Proměnné určuje proměnné konfigurace pro použití s automatickými uniformními klastry.

Atributy uvedené v sekci Proměnné můžete použít během automatické konfigurace klastru polí CONNAME a MQSC názvu kanálu příjemce klastru. Konfigurační proměnné nelze použít v žádném jiném prvku skriptu MQSC.

atribut=hodnota
Určuje název a přidruženou hodnotu pro použití jako vložení během definic MQSC.

Dvojice *atribut=hodnota* lze zadat pomocí volby příkazového řádku **-iv** v příkazu **crtmqm** při vytváření správce front.

Příklad stanza

```
Variables:
       CONNAME=127.0.0.1(1414)
```

Související pojmy

“Automatické vyvažování aplikací” na stránce 402
Automatické vyvažování aplikací výrazně rozšiřuje distribuci a dostupnost aplikací tím, že umožňuje jednotnému klastru IBM MQ pečlivě spravovat distribuci aplikací v rámci klastru a nespoléhat se na randomizaci ani na ruční připnutí aplikací ke specifickým správcům front.

Související úlohy

“Vytvoření nového uniformní klastru” na stránce 414
Jak vytvoříte nový jednotný klastr.

Související odkazy

“Použití automatické konfigurace klastru” na stránce 418
Produkt IBM MQ nakonfigurujete tak, aby umožňoval automatickou konfiguraci změnou informací o konfiguraci `qm.ini` .

Multi Sekce XAResourceManager souboru qm.ini

Sekce XAResourceManager určuje informace o správcích prostředků zapojených do globálních jednotek práce koordinovaných správcem front.

Prostřednictvím sekce XAResourceManager v souboru `qm.ini` můžete určit informace o správcích prostředků zapojených do globálních jednotek práce koordinovaných správcem front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front správce prostředků XA IBM MQ Explorer .

Přidejte informace o konfiguraci správce prostředků XA ručně pro každou instanci správce prostředků, která se účastní globálních pracovních jednotek; nejsou zadány žádné výchozí hodnoty.

Další informace o atributech správce prostředků naleznete v tématu Koordinace databáze .

Název = *název* (povinný)
Tento atribut identifikuje instanci správce prostředků.

Hodnota `Name` může mít délku až 31 znaků. Můžete použít název správce prostředků, jak je definován v jeho struktuře přepínače XA. Pokud však používáte více než jednu instanci stejného správce prostředků, musíte pro každou instanci vytvořit jedinečný název. Jedinečnost můžete zajistit například zahrnutím názvu databáze do řetězce `Name` .

IBM MQ používá hodnotu Name ve zprávách a ve výstupu příkazu dspmqtrn .

Neměňte název instance správce prostředků ani neodstraňujte její položku z konfiguračních informací po spuštění přidruženého správce front a po účinnosti názvu správce prostředků.

SwitchFile= *název* (povinné)
Úplný název zaváděcího souboru obsahujícího strukturu přepínače XA správce prostředků.

Používáte-li 64bitového správce front s 32bitovými aplikacemi, měla by hodnota name obsahovat pouze základní název zaváděcího souboru obsahujícího strukturu přepínače XA správce prostředků.

32bitový soubor bude načten do aplikace z cesty určené volbou ExitsDefaultPath.

64bitový soubor bude načten do správce front z cesty určené parametrem ExitsDefaultPath64.

XAOpenString= *řetězec* (volitelné)
Řetězec dat, která mají být předána 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 přistupovat. Další informace o definování tohoto atributu viz:

- Přidání informací o konfiguraci správce prostředků pro Db2
- Přidání informací o konfiguraci správce prostředků pro databázi Oracle
- Přidání informací o konfiguraci správce prostředků pro Sybase
- Přidání informací o konfiguraci správce prostředků pro Informix

a v dokumentaci ke správci prostředků vyhledejte příslušný řetězec.

XACloseString= *řetězec* (volitelné)
Řetězec dat, která mají být předána do vstupního bodu xa_close správce prostředků. Obsah řetězce závisí na samotném správci prostředků. Další informace o definování tohoto atributu viz:

- Přidání informací o konfiguraci správce prostředků pro Db2
- Přidání informací o konfiguraci správce prostředků pro databázi Oracle
- Přidání informací o konfiguraci správce prostředků pro Sybase
- Přidání informací o konfiguraci správce prostředků pro Informix

a v dokumentaci k databázi vyhledejte příslušný řetězec.

ThreadOfControl=THREAD | PROCESS
Windows Tento atribut je povinný pro Windows. Správce front používá tuto hodnotu pro serializaci, když potřebuje volat správce prostředků z jednoho ze svých vlastních procesů s podporou podprocesů.

Podproces
Správce prostředků plně *uvědomuje podprocesy*. V procesu IBM MQ s podporou podprocesů lze volání funkce XA provádět pro externího správce prostředků z více podprocesů současně.

PROCESS
Správce prostředků *nezabezpečuje podprocesy*. V procesu IBM MQ s podporou podprocesů lze ve správci prostředků provádět vždy pouze jedno volání funkce XA.

Položka **ThreadOfControl** se nevztahuje na volání funkcí XA vydaná správcem front v procesu aplikace s podporou podprocesů. Obecně platí, že aplikace, která má souběžné pracovní jednotky na různých podprocesech, vyžaduje, aby byl tento provozní režim podporován každým ze správců prostředků.

Příklad stanza

```
XAResourceManager:
   Name=DB2 Resource Manager Bank
   SwitchFile=/usr/bin/db2swit
   XAOpenString=MQBankDB
```

```
   XACloseString=
   ThreadOfControl=THREAD
```

Poznámka: Maximální počet sekcí XAResourceManager je omezen na 255. Měli byste však použít pouze malý počet sekcí, abyste se vyhnuli poklesu výkonu transakce.

IBM i Příklad souboru qm.ini pro IBM i

Příklad ukazující, jak mohou být skupiny atributů uspořádány v konfiguračním souboru správce front pro produkt IBM i.

```
#*******************************************************************#
#* Module Name: qm.ini                                             *#
#* Type       : IBM MQ queue manager configuration file            *#
# Function    : Define the configuration of a single queue manager *#
#*                                                                 *#
#*******************************************************************#
#* Notes      :                                                    *#
#* 1) This file defines the configuration of the queue manager     *#
#*                                                                 *#
#*******************************************************************#
Log:
LogPath=QMSATURN.Q
LogReceiverSize=65536

CHANNELS:
MaxChannels = 20       ; Maximum number of channels allowed.
                       ; Default is 100.
MaxActiveChannels = 10 ; Maximum number of channels allowed to be
                       ; active at any time. The default is the
                       ; value of MaxChannels.

TCP:                   ; TCP/IP entries.
KeepAlive = Yes        ; Switch KeepAlive on.
SvrSndBuffSize=20000   ; Size in bytes of the TCP/IP send buffer for each
                       ; channel instance. Default is 32768.
SvrRcvBuffSize=20000   ; Size in bytes of the TCP/IP receive buffer for each
                       ; channel instance. Default is 32768.
Connect_Timeout=10000  ; Number of seconds before an attempt to connect the
                       ; channel instance times out. Default is zero (no timeout).

QMErrorLog:
ErrorLogSize = 262144
ExcludeMessage = 7234
SuppressMessage = 9001,9002,9202
SuppressInterval = 30

TuningParameters:
   ImplSyncOpenOutput=2
```

ALW Konfigurační soubor instalace mqinst.ini

Na systémech AIX and Linux obsahuje konfigurační soubor instalace `mqinst.ini`informace o všech instalacích produktu IBM MQ . Na systémech Windows jsou informace o konfiguraci instalace v registru.

Umístění souboru `mqinst.ini`

Linux AIX

Soubor `mqinst.ini` se nachází v adresáři `/etc/opt/mqm` na systémech AIX and Linux . Obsahuje informace o tom, která instalace, pokud existuje, je primární instalací, a také následující informace pro každou instalaci:

- Název instalace
- Popis instalace
- Identifikátor instalace
- Instalační cesta

Důležité: Soubor `mqinst.ini` nesmí být upraven nebo odkazován přímo, protože jeho formát není pevný a mohl by se změnit.

Identifikátor instalace, pouze pro interní použití, je nastaven automaticky a nesmí být změněn.

Místo přímé úpravy souboru `mqinst.ini`musíte použít následující příkazy k vytvoření, odstranění, dotazování a úpravě hodnot v souboru:

crtmqinst -vytvoření položek.
dltmqinst pro odstranění položek.
dspmqinst pro zobrazení položek.
setmqinst pro nastavení položek.

Informace o konfiguraci instalace na systému Windows

Windows

V systému Windowsnení žádný soubor `mqinst.ini` . Informace o konfiguraci instalace jsou v registru a jsou uloženy v následujícím klíči:

```
HKLM\SOFTWARE\IBM\WebSphere MQ\Installation\InstallationName
```

Důležité: Tento klíč nesmí být upraven nebo odkazován přímo, protože jeho formát není pevný a mohl by se změnit.

Místo toho musíte použít následující příkazy k dotazování a úpravě hodnot v registru:

dspmqinst pro zobrazení položek.
setmqinst pro nastavení položek.

V systému Windowsnejsou příkazy **`crtmqinst`** a **`dltmqinst`** k dispozici. Procesy instalace a odinstalace zpracovávají vytvoření a odstranění požadovaných položek registru.

Multi IBM MQ MQI client konfigurační soubor mqclient.ini

Klienty můžete konfigurovat pomocí atributů v textovém souboru. Tyto atributy mohou být přepsány proměnnými prostředí nebo jinými způsoby specifickými pro platformu.

Produkt IBM MQ MQI clients konfigurujete pomocí textového souboru, který je podobný konfiguračnímu souboru správce front `qm.ini`. Soubor obsahuje počet sekcí, z nichž každý obsahuje počet řádků ve formátu **`attribute-name`** = *hodnota*.

Konfigurační soubor IBM MQ MQI client má obecně název `mqclient.ini` , ale můžete se rozhodnout, že mu dáte jiný název. Informace o konfiguraci v tomto souboru platí pro následující platformy:

- ALW AIX, Linux, and Windows
- IBM i IBM i

  Poznámka: V systému IBM ineexistuje žádný výchozí soubor `mqclient.ini` . Soubor však můžete vytvořit v souboru IBM i Integrated File System (IFS).

Další informace viz téma “Umístění konfiguračního souboru klienta” na stránce 157.

Poznámka: z/OS Platformu z/OS nelze použít ke spuštění klientů IBM MQ . Proto soubor `mqclient.ini` v systému IBM MQ for z/OSneexistuje.

Atributy v konfiguračním souboru IBM MQ MQI client platí pro klienty, kteří používají:

- Rozhraní MQI
- IBM MQ classes for Java
- IBM MQ classes for JMS
- IBM MQ classes for .NET

- XMS

Ačkoli atributy v konfiguračním souboru IBM MQ MQI client platí pro většinu klientů IBM MQ , existují některé atributy, které nejsou čteny spravovanými klienty .NET a XMS .NET nebo klienty, kteří používají buď IBM MQ classes for Java , nebo IBM MQ classes for JMS. Další informace viz “Kteří klienti IBM MQ mohou číst každý atribut” na stránce 158.

Funkce konfigurace se vztahují na všechna připojení, která aplikace klienta vytváří pro libovolné správce front, a nikoli na konkrétní připojení ke správci front. Atributy související s připojením k jednotlivému správci front lze konfigurovat programově, například pomocí struktury MQCD nebo pomocí tabulky CCDT (Client Channel Definition Table).

Zde je příklad konfiguračního souboru klienta:

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

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

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

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

LU62:
   TPName
   Library1=DLLName1
   Library2=DLLName2

PreConnect:
    Module=myMod
    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)

Connection:
     ApplName=ExampleApplName
```

Pomocí konfiguračního souboru klienta nelze nastavit připojení více kanálů.

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

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

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

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

Komentáře v konfiguračním souboru

Linux AIX

K označení začátku komentáře v konfiguračním souboru můžete použít středník ';' a znak hašování '#'. To může označit celý řádek jako komentář nebo označit komentář na konci řádku, který nebude zahrnut do hodnoty nastavení.

Pokud hodnota vyžaduje některý z těchto znaků, musíte tento znak změnit pomocí zpětného lomítka '\'.

Následující příklad ukazuje použití komentářů v konfiguračním souboru:

```
# Example of an SSL stanza with comments
SSL:
    ClientRevocationChecks=REQUIRED ; Example of an end of line comment
    SSLCryptoHardware=GSK_PKCS11=/driver\;label\;password\;SYMMETRIC_CIPHER_ON # Example of
escaped comment characters.
```

Související pojmy

Třídy IBM MQ pro konfigurační soubor Java

Multi Umístění konfiguračního souboru klienta

Konfigurační soubor IBM MQ MQI client lze zadržet v několika umístěních.

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

1. Umístění určené proměnnou prostředí **MQCLNTCF**.

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

   Notes:

   - Klienti C, .NET a XMS podporují pouze protokol `file:` ; protokol `file:` se předpokládá, pokud řetězec URL nezačíná na `protocol:`
   - Chcete-li povolit prostředí JRE Java 1.4.2 , která nepodporují čtení proměnných prostředí, lze proměnnou prostředí **MQCLNTCF** přepsat systémovou vlastností **MQCLNTCF** Java .
2. Soubor s názvem `mqclient.ini` v současném pracovním adresáři aplikace.
3. Soubor s názvem `mqclient.ini` v datovém adresáři IBM MQ pro systémy AIX, Linux, and Windows .

   Notes:

   - Datový adresář IBM MQ neexistuje na určitých platformách, například IBM i a z/OS, nebo v případech, kdy byl klient dodán s jiným produktem.

     IBM i V systému IBM ineexistuje žádný výchozí soubor `mqclient.ini` . Avšak soubor lze vytvořit v systému IBM i Integrated File System) v adresáři `/QIBM/UserData/mqm/`a proměnnou prostředí **MQCLNTCF** definovanou tak, aby na něj ukazovala. Příklad:

     ```
     ADDENVVAR ENVVAR(MQCLNTCF) VALUE('QIBM/UserData/mqm/mqclient.ini') REPLACE(*YES)
     ```

     Další příklady proměnných prostředí viz “Popisy proměnných prostředí” na stránce 63.

     z/OS Platformu z/OS nelze použít ke spuštění klientů IBM MQ . Proto soubor `mqclient.ini` v systému IBM MQ for z/OSneexistuje.
   - Linux AIX Na systémech AIX and Linux je adresář `/var/mqm`.
   - Windows Na platformách Windows konfigurujte proměnnou prostředí **MQ_DATA_PATH** během instalace tak, aby ukazovala na datový adresář. Obvykle se jedná o `C:\ProgramData\IBM\MQ.`

     Poznámka: Pokud instalujete pouze klienta, proměnná prostředí může být **MQ_FILE_PATH**.

- Chcete-li povolit prostředí JRE Java 1.4.2 , která nepodporují čtení proměnných prostředí, můžete ručně přepsat proměnnou prostředí **MQ_DATA_PATH** systémovou vlastností **MQ_DATA_PATH** Java .

4. Soubor s názvem `mqclient.ini` ve standardním adresáři odpovídajícím platformě a přístupný uživatelům:
   - Pro všechny klienty Java je to hodnota systémové vlastnosti `user.home` Java .
   - Linux AIX Pro klienty C na platformách AIX and Linux se jedná o hodnotu proměnné prostředí **HOME** .
   - Windows Pro klienty C v systému Windows se jedná o zřetězené hodnoty proměnných prostředí **HOMEDRIVE** a **HOMEPATH** .

Multi Kteří klienti IBM MQ mohou číst každý atribut

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

Tabulka 15. Které atributy platí pro každý typ klienta

`mqclient.ini` název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
STANZA kanálů						
CCSID	Číslo kódované znakové sady, které se má použít.	Ano	Ne	Ne	Ano	Ano
ChannelDefinitionAdresář	Cesta k adresáři se souborem obsahujícím tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano
ChannelDefinitionSoubor	Název souboru obsahujícího tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
ReconDelay	Administrativní volba pro konfiguraci prodlevy opětovného připojení pro klientské programy, které se mohou automaticky znovu připojit.	Ano	Ne	Ano	Ano	Ano
DefRecon	Administrativní volba, která umožňuje klientským programům automatické opětovné připojení nebo zakázání automatického opětovného připojení klientského programu, který byl napsán pro automatické opětovné připojení.	Ano	Ne	Ano	Ano	Ano
MQReconnectTimeout	Časový limit v sekundách pro opětovné připojení ke klientovi.	Ano	Ne	Ne	Ano	Ne
ServerConnectionparametry	Umístění serveru IBM MQ a komunikační metoda, která se má použít.	Ano	Ne	Ne	Ano	Ano

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
Put1DefaultAlwaysSync	Řídí chování volání funkce MQPUT1 s volbou MQPMO_RESPONSE_AS_Q_DEF.	Ano	Ano	Ano	Ano	Ano
PasswordProtection	Umožňuje vám nastavit chráněná hesla ve struktuře MQCSP namísto použití SSL nebo TLS.	Ano	Ano	Ano	Ano	Ano
ClientExitSekce cesty						
ExitsDefaultPath	Určuje umístění 32bitových uživatelských procedur kanálu pro klienty.	Ano	Ano	Ano	Ano	Ano
ExitsDefaultPath64	Určuje umístění 64bitových uživatelských procedur kanálu pro klienty.	Ano	Ano	Ano	Ano	Ano
JavaExitsClassPath	Hodnoty, které se mají přidat do cesty ke třídě při spuštění uživatelské procedury Java .	Ne	Ano	Ano	Ne	Ne
Sekce připojení						
ApplName	Název aplikace uvedený v konfiguračním souboru klienta.	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
Sekce JMQI						
useMQCSPauthentication	Určuje, zda mají aplikace IBM MQ classes for Java a IBM MQ classes for JMS při ověřování se správcem front používat režim kompatibility nebo režim ověřování MQCSP.	Ne	Ano	Ano	Ne	Ne
MessageBuffer sekce						
MaximumSize	Velikost vyrovnávací paměti pro čtení napřed v kilobajtech v rozsahu 1 až 999 999.	Ano	Ano	Ano	Ano	Ano
PurgeTime	Interval v sekundách, po jehož uplynutí jsou zprávy zanechané ve vyrovnávací paměti dopředného čtení vymazány.	Ano	Ano	Ano	Ano	Ano

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)						
mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
UpdatePercentage	Procentní hodnota aktualizace v rozsahu 1-100 použitá při výpočtu prahové hodnoty k určení, kdy aplikace klienta vytvoří nový požadavek na server.	Ano	Ano	Ano	Ano	Ano
PreConnect stanza						
Data	Adresa URL úložiště, kde jsou uloženy definice připojení.	Ano	Ne	Ne	Ne	Ne
funkce	Název funkčního vstupního bodu do knihovny, která obsahuje kód ukončení PreConnect .	Ano	Ne	Ne	Ne	Ne
Modul	Název modulu obsahujícího kód uživatelské procedury rozhraní API.	Ano	Ne	Ne	Ne	Ne
Posloupnost	Posloupnost, ve které je tato uživatelská procedura volána vzhledem k jiným uživatelským procedurám.	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
Sekce zabezpečení						
DisableClientAMS	Zakáže nebo povolí produkt AMS pro připojení klienta ke správci front.	Ano	Ano	Ano	Ne	Ne
Sekce SSL						
V 9.3.0 OutboundSNI	Uvádí, zda klienti s podporou SNI nastaví SNI na název cílového kanálu IBM MQ pro vzdálený systém při inicializaci připojení TLS nebo na název hostitele.	Ano	Ano	Ano	Ano	Ne
AllowOutboundSNI	Uvádí, zda klienti s podporou SNI nastaví SNI na název cílového kanálu IBM MQ pro vzdálený systém při inicializaci připojení TLS. **Upozornění:** Deprecated V 9.3.0 Od IBM MQ 9.3.0 je tato vlastnost zamítnuta. Místo toho použijte **OutboundSNI** .	Ano	Ano	Ano	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
AllowTLSV13	Zda může správce front používat specifikace TLS 1.3 CipherSpecs.	Ano (klienti C/C++)	Ne	Ne	Ne	Ne
CDPCheckExtensions	Určuje, zda se kanály SSL nebo TLS v tomto správci front pokusí zkontrolovat servery CDP, které jsou uvedeny v rozšířeních certifikátu CrlDistributionPoint.	Ano	Ne	Ne	Ne	Ne
CertificateLabel	Popisek certifikátu definice kanálu.	Ano	Ne	Ne	Ne	Ne
CertificateVal	Určuje typ použitého ověření platnosti certifikátu.	Ano	Ne	Ne	Ne	Ne
ClientRevocation	Určuje, jak je konfigurována a kontrola odvolání certifikátů, pokud volání připojení klienta používá kanál SSL/TLS.	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
EncryptionPolicySuiteB	Určuje, zda kanál používá šifrování vyhovující standardu Suite-B a jakou úroveň síly má být použita.	Ano	Ne	Ne	Ne	Ne
V 9.3.0 EnvironmentScope	Řídí, zda produkt IBM MQ používá jediné prostředí IBM Global Security Kit (GSKit) pro celý proces nebo prostředí GSKit pro každé připojení.	Ano (klienti C)	Ne	Ne	Ne	Ne
MinimumRSAKeyVelikost	Uvádí minimální velikost klíče, kterou musí mít certifikáty RSA, aby mohly být přijaty.	Ano (klienti C/C++)	Ne	Ne	Ne	Ne
OCSPAuthentication	Definuje chování produktu IBM MQ , když je povolen protokol OCSP a kontrola odvolání protokolu OCSP nemůže určit stav odvolání certifikátu.	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
OCSPCheckExtensions	Řídí, zda produkt IBM MQ pracuje s rozšířeními certifikátu AuthorityInfo Access.	Ano	Ne	Ne	Ne	Ne
OCSPTimeout	Počet sekund čekání na odpovídací modul OCSP při provádění kontroly odvolání.	Ano	Ne	Ne	Ne	Ne
ALW PeerCertChainValidation	Nastavení ověření platnosti certifikátu GSKit .	Ano	Ne	Ne	Ne	Ne
SSLCryptoHardware	Nastaví řetězec parametrů nezbytný pro konfiguraci šifrovacího hardwaru PKCS #11 přítomného v systému.	Ano	Ne	Ne	Ne	Ne
SSLCryptoHardwareKeyFile	Uvádí úplnou cestu a název souboru obsahujícího počáteční klíč, který byl použit k zašifrování hesla v řetězci konfigurace šifrovacího hardwaru PKCS #11 , který je uveden s atributem **SSLCryptoHardware** .	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
SSLFipsRequired	Uvádí, zda se mají použít pouze algoritmy certifikované FIPS, pokud se šifrování provádí v produktu IBM MQ.	Ano	Ne	Ne	Ne	Ne
SSLHTTPProxyName	Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má produkt GSKit použít pro kontroly OCSP.	Ano	Ne	Ne	Ne	Ne
SSLHTTPConnectTimeout	Počet sekund čekání na úspěšné vytvoření síťového připojení k serveru HTTP při provádění kontroly odvolání.	Ano	Ne	Ne	Ne	Ne
SSLKeyRepository	Umístění úložiště klíčů, které obsahuje digitální certifikát uživatele, v kmenovém formátu.	Ano	Ne	Ne	Ne	Ne
V 9.3.0 V 9.3.0 SSLKeyRepositoryHeslo	Přístupová fráze pro přístup k úložišti klíčů.	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
SSLKeyResetPočet	Počet nešifrovaných bajtů odeslaných a přijatých na kanálu SSL nebo TLS, než je znovu vyjednán tajný klíč.	Ano	Ne	Ne	Ne	Ne
stanza TCP						
ClntRcvBuffSize	Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech, kterou používá klientský konec kanálu připojení serveru pro připojení klienta.	Ano	Ano	Ano	Ano	Ano
ClntSndBuffSize	Velikost odesílací vyrovnávací paměti TCP/IP v bajtech, kterou používá klientský konec kanálu připojení serveru připojení klienta.	Ano	Ano	Ano	Ano	Ano
Časový limit připojení	Počet sekund do vypršení časového limitu pokusu o připojení soketu.	Ano	Ano	Ano	Ne	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)

mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
IPAddressVersion	Určuje, který protokol IP má být použit pro připojení kanálu.	Ano	Ne	Ne	Ano	Ano
KeepAlive	Zapne nebo vypne funkci KeepAlive .	Ano	Ano	Ano	Ano	Ano
Windows Library1	Pouze v systému Windows se jedná o název knihovny DLL soketů TCP/IP.	Ano	Ne	Ne	Ne	Ne
Sekce trasování **Poznámka:** Sekce trasování se vztahuje pouze na klienty IBM MQ .NET a XMS .NET .						
V 9.3.3 MQDotnetTraceÚroveň	Používá se k povolení trasování produktu IBM MQ .NET .	Ne	Ne	Ne	Ano	Ne
V 9.3.3 MQDotnetTraceCesta	Ukazuje na složku, kde budou vytvořeny trasovací soubory produktu IBM MQ .NET .	Ne	Ne	Ne	Ano	Ne
V 9.3.3 MQDotnetErrorCesta	Ukazuje na složku, kde budou vytvořeny soubory protokolu chyb pro trasování produktu IBM MQ .NET .	Ne	Ne	Ne	Ano	Ne

Tabulka 15. Které atributy platí pro každý typ klienta (pokračování)						
mqclient.ini název a atributy sekce	**Popis**	**C a nespravovaný .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
V 9.3.3 XMSDotnetTraceÚroveň	Používá se k povolení trasování XMS .NET .	Ne	Ne	Ne	Ne	Ano
V 9.3.3 XMSDotnetTraceFilePath	Ukazuje na složku, kde budou vytvořeny trasovací soubory XMS .NET .	Ne	Ne	Ne	Ne	Ano
V 9.3.3 XMSDotnetTraceSpecifikace	Uvádí název třídy, kterou chcete trasovat pro XMS .NET.	Ne	Ne	Ne	Ne	Ano
V 9.3.3 XMSDotnetTraceSpecifikace	Uvádí maximální velikost trasovacího souboru, který by měl být generován pro XMS .NET.	Ne	Ne	Ne	Ne	Ano
V 9.3.3 XMSDotnetTraceFileSize	Počet trasovacích souborů, které se mají uchovat pro XMS .NET.	Ne	Ne	Ne	Ne	Ano

V 9.3.0 `Application` sekce konfiguračního souboru klienta

Sekci `Application` použijte k určení atributů, které ovlivňují chování rovnoměrného vyvážení klastru pro specifickou aplikaci připojující se pomocí této konfigurace. Hodnoty v této sekci mají přednost před sekcí `ApplicationDefaults` , ale mohou být přepsány strukturou MQBNO poskytnutou prostřednictvím programu.

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

Následující atributy lze zahrnout do sekce Aplikace:

Název = `ApplicationName`
Identifikuje, na který název aplikace se volby vztahují.

Typ = *Jednoduchý,ReqRep*
Označuje IBM MQ obecný vzor aktivity IBM MQ , které se tato aplikace účastní.

BalanceTimeout = *Never,Immediate,0-999999999, výchozí*
Označuje IBM MQ časový limit, než může být aktivita aplikace přerušena, aby bylo možné znovu vybalancovat; buď nikdy, nebo hodnota až do maxima 999999999 sekund, s výchozí hodnotou 10 sekund.

BalanceOptions = *Žádný,IgnTrans*
Buď nejsou nastaveny žádné volby vyvažování, nebo povolují okamžité přerušení aplikací, které jsou momentálně zapojeny do transakce.

Multi V 9.3.0 `ApplicationDefaults` sekce konfiguračního souboru klienta

Pomocí sekce `ApplicationDefaults` určete atributy, které ovlivňují výchozí chování rovnoměrného vyvážení klustru pro klientské aplikace, které se připojují pomocí této konfigurace. Tato výchozí nastavení mohou být přepsána buď sekcí `Application` specifickou pro aplikaci, nebo strukturou MQBNO poskytnutou prostřednictvím programu.

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

Následující atributy lze zahrnout do sekce ApplicationDefaults :

Typ = *Jednoduchý,ReqRep*
Označuje IBM MQ obecný vzor aktivity IBM MQ , které se tato aplikace účastní.

BalanceTimeout = *Never,Immediate,0-999999999, výchozí*
Označuje IBM MQ časový limit, než může být aktivita aplikace přerušena, aby bylo možné znovu vybalancovat; buď nikdy, nebo hodnota až do maxima 999999999 sekund, s výchozí hodnotou 10 sekund.

BalanceOptions = *Žádný,IgnTrans*
Buď nejsou nastaveny žádné volby vyvažování, nebo povolují okamžité přerušení aplikací, které jsou momentálně zapojeny do transakce.

Multi Sekce kanálů konfiguračního souboru klienta

Sekci Kanály použijte k uvedení informací o kanálech klienta.

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

V sekci Kanály lze zahrnout následující atributy:

CCSID = *číslo*
Číslo kódované znakové sady, které se má použít.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, spravovaní klienti .NETa spravovaní klienti XMS .NET .

Číslo CCSID je ekvivalentní proměnné prostředí MQCCSID .

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

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, spravovaní klienti .NETa spravovaní klienti XMS .NET .

Windows Na systémech Windows je výchozí adresář dat a souborů protokolu IBM MQ , obvykle `C:\ProgramData\IBM\MQ`.

Linux AIX Na systémech AIX and Linux je výchozí hodnota `/var/mqm`.

ChannelDefinitionAdresář může obsahovat URL , která pracuje v kombinaci s atributem ChannelDefinition(viz “Přístup URL k tabulce CCDT” na stránce 52).

Cesta k adresáři ChannelDefinitionje ekvivalentní proměnné prostředí **MQCHLLIB** .

ChannelDefinitionSoubor = *název souboru*|AMQCLCHL.TAB
Název souboru obsahujícího tabulku definic kanálů klienta.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, spravovaní klienti .NETa spravovaní klienti XMS .NET .

Tabulka definic kanálů klienta je ekvivalentní proměnné prostředí **MQCHLTAB** .

ReconDelay = (delay [, rand]) (delay [, rand]) ...
Atribut ReconDelay poskytuje administrativní volbu pro konfiguraci prodlevy opětovného připojení pro klientské programy, které se mohou automaticky znovu připojit.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Zde je příklad konfigurace:

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

Zobrazený příklad definuje počáteční prodlevu jedné sekundy plus náhodný interval až 200 milisekund. Další prodleva je dvě sekundy plus náhodný interval až 200 milisekund. Všechna následná zpoždění jsou čtyři sekundy plus náhodný interval až 1000 milisekund.

DefRecon = NO|YES|QMGR|DISABLED
Atribut DefRecon poskytuje administrativní volbu, která umožňuje klientským programům automaticky se znovu připojit nebo zakázat automatické opětovné připojení klientského programu, který byl napsán, aby se znovu automaticky připojil. Pokud program používá volbu, například MQPMO_LOGICAL_ORDER, která je nekompatibilní s opětovným připojením, můžete zvolit její nastavení.

Tento atribut může číst C, nespravovaní klienti .NET, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Automatické opětovné připojení klienta není podporováno produktem IBM MQ classes for Java.

Automatické opětovné připojení klienta obvykle závisí na dvou hodnotách, které jsou:

- Volba opětovného připojení nastavená v aplikaci MQCONNX (nebo továrně připojení JMS)
- Výchozí volba opětovného připojení dodaná v libovolné používané definici připojení klienta (struktura MQCD, například dodávaná pomocí souboru CCDT).

Atribut `mqclient.ini` file platí **pouze** , pokud není použita žádná definice kanálu, která nastaví atribut **DefReconnect** a v této situaci se chová, jako by byla dodána. Atribut kanálu **DefReconnect** (a tedy tento atribut, je-li použitelný):

- Potlačit kód aplikace, je-li některá z těchto možností nastavena na hodnotu DISABLED.
- Jsou potlačeny kódem aplikace ve všech ostatních případech, pokud jsou zadány volby v MQCONNX.

Viz popis DEFRECON pro tabulku zobrazující všechny možné kombinace aplikací a dodaných hodnot definice kanálu.

Notes:

- Pokud se používá MQCD, ale je před datem MQCD_VERSION_10, parametr **DefReconnnect** není součástí struktury. V této situaci se hodnota chybějícího parametru naplní hodnotou `mqclient.ini` soubor **DefReconnnect** , pokud je uvedena. K tomu může dojít například v případě, že klientská aplikace stále používá binární formát CCDT vygenerovaný ve starší verzi produktu IBM MQ .
- Při interpretaci kódu klienta IBM MQ tabulka JSON CCDT, viz “Konfigurace formátu JSON CCDT” na stránce 44, vždy generuje struktury MQCD v nejnovější verzi, a proto vždy dodává výchozí hodnotu (NO) pro tento atribut, pokud není explicitně uvedena jiná hodnota.

MQReconnectTimeout

Maximální doba v sekundách, po kterou se funkce automatického opětovného připojení klienta v klientovi pokusí znovu navázat připojení. Výchozí hodnota je 1800 sekund (30 minut).

Tento atribut mohou číst klienti C a nespravovaní klienti .NET a spravovaní klienti .NET .

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

Klienti IBM MQ classes for XMS .NET mohou zadat časový limit pro opětovné připojení pomocí následujících vlastností:

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

Parametry ServerConnection

Parametr ServerConnectionje ekvivalentní proměnné prostředí *MQSERVER* a určuje umístění serveru IBM MQ a komunikační metodu, která se má použít.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, spravovaní klienti .NETa spravovaní klienti XMS .NET .

Atribut ServerConnectionParms definuje pouze jednoduchý kanál. Nelze jej použít k definování kanálu TLS nebo kanálu s ukončením kanálu. Jedná se o řetězec ve formátu *ChannelName*/*TransportType*/*ConnectionName*, *ConnectionName* musí být úplný název sítě. *ChannelName* nesmí obsahovat dopředné lomítko (/), protože tento znak slouží k oddělení názvu kanálu, typu transportu a názvu připojení.

Při použití parametrů ServerConnectionk definování kanálu klienta je použita maximální délka zprávy 100 MB. Proto je maximální velikost zprávy platná pro kanál hodnotou určenou v kanálu SVRCONN na serveru.

Povšimněte 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)
```

Použije se pouze druhý.

Zadejte *ConnectionName* jako seznam názvů pro uvedený typ přenosu oddělených čárkami. Obecně je vyžadován pouze jeden název. Chcete-li konfigurovat více připojení se stejnými vlastnostmi, můžete zadat více *názvů hostitelů* . Připojení jsou zkoušena v pořadí, v jakém jsou uvedena v seznamu připojení, dokud není připojení úspěšně zavedeno. Není-li připojení úspěšné, klient začne znovu zpracovávat. Seznamy připojení jsou alternativou ke skupinám správců front pro konfiguraci připojení pro klienty s možností opětovného připojení.

Put1DefaultAlwaysSync = NO (výchozí) | YES

Řídí chování volání funkce MQPUT1 s volbou MQPMO_RESPONSE_AS_Q_DEF.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

NO

Je-li volba MQPUT1 nastavena na hodnotu MQPMO_SYNCPOINT, chová se jako MQPMO_ASYNC_RESPONSE. Podobně, je-li volba MQPUT1 nastavena na hodnotu MQPMO_NO_SYNCPOINT, chová se jako MQPMO_SYNC_RESPONSE. Toto je výchozí hodnota.

YES

MQPUT1 se chová, jako by byl nastaven parametr MQPMO_SYNC_RESPONSE , bez ohledu na to, zda je nastaven parametr MQPMO_SYNCPOINT nebo MQPMO_NO_SYNCPOINT .

PasswordProtection = Kompatibilní (výchozí) |vždy|volitelné

V produktu IBM MQ 8.0lze ověřovací pověření, která aplikace IBM MQ client zadávají při připojení ke správci front, chránit pomocí funkce ochrany heslem produktu IBM MQ MQCSP, pokud připojení nepoužívá šifrování TLS.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Ochrana heslem MQCSP je užitečná pro účely testování a vývoje, protože použití ochrany heslem MQCSP je jednodušší než nastavení šifrování TLS, ale ne tak bezpečné.

Další informace o ochraně pověření ve struktuře MQCSP a hodnotách, které lze nastavit pro tento atribut, naleznete v tématu Ochrana heslem MQCSP.

Související úlohy

Připojení aplikací MQI IBM MQ ke správcům front

Multi ClientExitSekce cesty konfiguračního souboru klienta

Sekci cesty ClientExitpoužijte k určení výchozích umístění uživatelských procedur kanálu na klientovi.

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

Do sekce ClientExitPath lze zahrnout následující atributy:

ExitsDefaultCesta = *řetězec*
Určuje umístění 32bitových uživatelských procedur kanálu pro klienty.

Tento atribut může číst klienti C, nespravovaní klienti .NET, spravovaní .NET, spravovaní XMS .NET, IBM MQ classes for Javaa IBM MQ classes for JMS . Klienti IBM MQ classes for Java a IBM MQ classes for JMS používají tento atribut k vyhledání 32bitových uživatelských procedur kanálu, které nejsou zapsány v souboru Java.

ExitsDefaultPath64 = *řetězec*
Určuje umístění 64bitových uživatelských procedur kanálu pro klienty.

Tento atribut může číst klienti C, nespravovaní klienti .NET, spravovaní .NET, spravovaní XMS .NET, IBM MQ classes for Javaa IBM MQ classes for JMS . Klienti IBM MQ classes for Java a IBM MQ classes for JMS používají tento atribut k vyhledání 64bitových uživatelských procedur kanálu, které nejsou zapsány v souboru Java.

JavaExitsClassPath = *řetězec*
Hodnoty, které se mají přidat do cesty ke třídě při spuštění uživatelské procedury Java . Toto je ignorováno ukončením v jakémkoli jiném jazyce.

Tento atribut mohou číst klienti IBM MQ classes for Java a IBM MQ classes for JMS .

V konfiguračním souboru JMS je názvu cesty JavaExitsClassposkytnut standardní com.ibm.mq.cfg. předpona a tento úplný název se také používá v systémové vlastnosti IBM MQ .

Multi Sekce připojení konfiguračního souboru klienta

K určení názvu aplikace použijte sekci připojení.

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

Následující atribut lze zahrnout do sekce Připojení:

ApplName = ExampleApplname
V konfiguračním souboru klienta můžete zadat název aplikace.

Tento atribut mohou používat klienti C a nespravovaní klienti .NET .

Multi Sekce JMQI konfiguračního souboru klienta

Pomocí sekce JMQI určete konfigurační parametry pro rozhraní Java Message Queuing Interface (JMQI) používané IBM MQ classes for Java a IBM MQ classes for JMS.

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

Následující atribut lze zahrnout do sekce JMQI:

useMQCSPauthentication = NO|YES
Určuje, zda mají aplikace IBM MQ classes for Java a IBM MQ classes for JMS při ověřování se správcem front používat režim kompatibility nebo režim ověřování MQCSP.

Tento atribut mohou číst klienti IBM MQ classes for Javaa IBM MQ classes for JMS .

Tento atribut může mít následující hodnoty:

NO
Při ověřování se správcem front použijte režim kompatibility. Jedná se o výchozí hodnotu ve verzích starších než IBM MQ 9.3.0.

YES
Při ověřování se správcem front používejte režim ověřování MQCSP. V 9.3.0 Toto je výchozí hodnota z IBM MQ 9.3.0.

Existuje několik dalších způsobů, jak nastavit režim ověření, které mají přednost před hodnotou atributu **useMQCSPauthentication** . Další informace o režimu kompatibility a režimu ověřování MQCSP naleznete v tématu Ověřování připojení pomocí Java klienta.

Windows Sekce LU62, NETBIOS a SPX konfiguračního souboru klienta

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

Sekce LU62

Pomocí sekce LU62 zadejte konfigurační parametry protokolu SNA LU 6.2 . Do této sekce lze zahrnout následující atributy:

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

Library2 = *DLLName*|WCPIC32
Totéž jako Library1, používá-li se kód uložený ve dvou samostatných knihovnách.

TPName
Název TP, který se má spustit na vzdáleném serveru.

Stanza systému NETBIOS

Použijte sekci NETBIOS k uvedení konfiguračních parametrů protokolu NetBIOS . Do této sekce lze zahrnout následující atributy:

AdapterNum = *číslo*|0
Číslo adaptéru LAN.

Library1 = *DLLName*|NETAPI32
Název knihovny DLL NetBIOS .

LocalName = *název*
Název, pod kterým je tento počítač v síti LAN známý.

Jedná se o ekvivalent proměnné prostředí MQNAME .

NumCmds = *číslo*|1
Kolik příkazů přidělit.

NumSess = *číslo*|1
Kolik relací se má přidělit.

Sekce SPX

Pomocí sekce SPX zadejte konfigurační parametry protokolu SPX. Do této sekce lze zahrnout následující atributy:

BoardNum = *číslo*|0
Číslo adaptéru LAN.

KeepAlive = YES|NO
Zapněte nebo vypněte funkci KeepAlive .

KeepAlive = YES způsobuje, že SPX pravidelně kontroluje, zda je druhý konec připojení stále k dispozici. Pokud není, kanál se zavře.

Library1 = *DLLName*|WSOCK32.Knihovna DLL
Název knihovny DLL SPX.

Library2 = *DLLName*|WSOCK32.Knihovna DLL
Totéž jako Library1, používá-li se kód uložený ve dvou samostatných knihovnách.

Soket = *číslo*|5E86
Číslo soketu SPX v hexadecimální notaci.

Multi Sekce MessageBuffer konfiguračního souboru klienta

Pomocí sekce MessageBuffer zadejte informace o vyrovnávacích pamětech zpráv.

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

Následující atributy lze zahrnout do sekce MessageBuffer :

MaximumSize = *celé číslo*|1
Velikost vyrovnávací paměti pro čtení napřed v kilobajtech v rozsahu 1 až 999 999.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Existují následující speciální hodnoty:

-1
Klient určí odpovídající hodnotu.

0
Dopředné čtení je pro klienta zakázáno.

PurgeTime = *celé číslo*|600
Interval v sekundách, po jehož uplynutí jsou zprávy zanechané ve vyrovnávací paměti dopředného čtení vymazány.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Pokud klientská aplikace vybírá zprávy na základě MsgId nebo CorrelId , je možné, že vyrovnávací paměť dopředného čtení může obsahovat zprávy odeslané klientovi s dříve požadovaným MsgId nebo CorrelId. Tyto zprávy by pak byly zadrženy ve vyrovnávací paměti dopředného čtení, dokud nebude vydán příkaz MQGET s příslušným MsgId nebo CorrelId. Zprávy z vyrovnávací paměti dopředného čtení můžete vymazat nastavením volby PurgeTime. Všechny zprávy, které zůstaly ve vyrovnávací paměti dopředného čtení po dobu delší, než je interval vymazání, jsou automaticky vymazány. Tyto zprávy již byly odebrány z fronty ve správci front, takže pokud nejsou procházeny, jsou ztraceny.

Platný rozsah je v rozsahu 1 až 999 999 sekund nebo speciální hodnota 0, což znamená, že nedojde k žádnému vymazání.

UpdatePercentage = *celé číslo*|-1

Procentní hodnota aktualizace v rozsahu 1-100 použitá při výpočtu prahové hodnoty k určení, kdy aplikace klienta vytvoří nový požadavek na server. Speciální hodnota -1 označuje, že klient určí odpovídající hodnotu.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Klient pravidelně odesílá na server požadavek s informací o tom, kolik dat klientská aplikace spotřebovala. Požadavek je odeslán, když počet bajtů *n*načtených klientem prostřednictvím volání MQGET překročí prahovou hodnotu *T*. Hodnota *n* se resetuje na nulu při každém odeslání nového požadavku na server.

Prahová hodnota T se vypočítá takto:

```
T = Upper - Lower
```

Horní hodnota je stejná jako velikost vyrovnávací paměti pro dopředné čtení určená atributem *MaximumSize* v kilobajtech. Výchozí hodnota je 100 kB.

Nižší hodnota je nižší než horní hodnota a je určena atributem *UpdatePercentage* . Tento atribut je číslo v rozsahu 1 až 100 a má výchozí hodnotu 20. Dolní hodnota se vypočítá takto:

```
Lower = Upper x UpdatePercentage / 100
```

Příklad 1:

Atributy MaximumSize a UpdatePercentage mají výchozí hodnotu 100 kB a 20 kB.

Klient volá příkaz MQGET, aby načetl zprávu, a to opakovaně. Tato operace pokračuje, dokud příkaz MQGET nespotřebuje n bajtů.

Použití výpočtu

```
T = Upper - Lower
```

T je (100-20) = 80 Kb.

Takže když volání MQGET odebrala 80 kB z fronty, klient automaticky vytvoří nový požadavek.

Příklad 2:

Atributy MaximumSize mají výchozí hodnotu 100 kB a pro hodnotu UpdatePercentageje vybrána hodnota 40.

Klient volá příkaz MQGET, aby načetl zprávu, a to opakovaně. Tato operace pokračuje, dokud příkaz MQGET nespotřebuje n bajtů.

Použití výpočtu

```
T = Upper - Lower
```

T je (100-40) = 60 Kb

Takže když volání MQGET odebrala 60 kB z fronty, klient automaticky vytvoří nový požadavek. Toto je dříve než v PŘÍKLADU 1, kde byly použity výchozí hodnoty.

Proto má volba větší prahové hodnoty *T* tendenci snižovat frekvenci odesílání požadavků z klienta na server. Naopak výběr menší prahové hodnoty *T* má tendenci zvyšovat frekvenci požadavků odesílaných z klienta na server.

Výběr velké prahové hodnoty *T* však může znamenat, že zvýšení výkonu dopředného čtení se sníží, protože pravděpodobnost, že vyrovnávací paměť dopředného čtení bude prázdná, se může zvýšit. Pokud k tomu dojde, může být nutné pozastavit volání MQGET a čekat na příchod dat ze serveru.

Multi Sekce PreConnect konfiguračního souboru klienta

Sekci PreConnect použijte ke konfiguraci uživatelské procedury PreConnect v souboru `mqclient.ini` .

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

Následující atributy lze zahrnout do sekce PreConnect :

Data = *user_data*
Tento atribut určuje uživatelská data, která jsou předána uživatelské proceduře pro předběžné připojení. Data předaná uživatelské proceduře předběžného připojení jsou specifická pro implementaci uživatelské procedury předběžného připojení, kterou používáte, a jaká data mají být předána.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Tento atribut lze například použít k určení URL úložiště, kde jsou uloženy definice připojení, například při použití serveru LDAP:

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

Funkce = *myFunc*
Název funkčního vstupního bodu do knihovny, která obsahuje kód ukončení PreConnect .

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Definice funkce dodržuje prototyp ukončení PreConnect MQ_PRECONNECT_EXIT.

Maximální délka tohoto pole je MQ_EXIT_NAME_LENGTH.

Module = *myMod*
Název modulu obsahujícího kód uživatelské procedury rozhraní API.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Pokud toto pole obsahuje úplný název cesty k modulu, použije se tak, jak je.

Pořadové číslo = *číslo_posloupnosti*
Posloupnost, ve které je tato uživatelská procedura volána vzhledem k jiným uživatelským procedurám. Ukončení s nízkým pořadovým číslem je voláno před ukončením s vyšším pořadovým číslem. Není třeba, aby pořadové číslo východů bylo spojité; posloupnost 1, 2, 3 má stejný výsledek jako posloupnost 7, 42, 1096. Tento atribut je číselná hodnota bez znaménka.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

V souboru `mqclient.ini` lze definovat více sekcí PreConnect . Pořadí zpracování každé uživatelské procedury je určeno atributem Sequence sekce.

Související úlohy
Odkazování na definice připojení pomocí uživatelské procedury před připojením z úložiště

Multi Sekce zabezpečení konfiguračního souboru klienta

Pomocí sekce Zabezpečení můžete zakázat nebo povolit produkt AMS pro připojení klienta ke správci front.

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

Následující atribut lze zahrnout do sekce Zabezpečení:

DisableClientAMS = NO|YES

Atribut DisableClientAMS vám umožňuje zakázat IBM MQ Advanced Message Security (AMS), pokud používáte klienta IBM MQ pro připojení ke správci front z dřívější verze produktu a je ohlášena chyba `2085 (MQRC_UNKNOWN_OBJECT_NAME)`.

Funkce IBM MQ Advanced Message Security (AMS) je automaticky povolena v klientu IBM MQ , a proto se klient standardně pokouší zkontrolovat zásady zabezpečení pro objekty ve správci front.

Následující příklady ukazují, jak používat atribut DisableClientAMS :

- Chcete-li zakázat AMS:

```
Security:
DisableClientAMS=Yes
```

- Chcete-li povolit AMS:

```
Security:
DisableClientAMS=No
```

Tento atribut mohou číst klienti C, IBM MQ classes for Javaa IBM MQ classes for JMS .

V 9.3.0 V 9.3.0 **MQIInitialKeySoubor = *pathname***

Úplná cesta a název souboru obsahujícího počáteční klíč, který byl použit k šifrování pověření poskytnutých klientem. Počáteční klíč musí být uveden, pokud byl uveden počáteční soubor s klíči, když byla přístupová fráze úložiště klíčů zašifrována pomocí obslužného programu **runmqicred** .

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Související úlohy

Zakázání rozšířeného zabezpečení zpráv na klientovi

Multi Sekce SSL konfiguračního souboru klienta

Pomocí sekce SSL uveďte informace o použití TLS.

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

Následující atributy lze zahrnout do sekce SSL:

V 9.3.0 **OutboundSNI = CHANNEL | HOSTNAME**

Je-li parametr **OutboundSNI** nastaven na hodnotu CHANNEL, klienti s podporou SNI nastaví při inicializaci připojení TLS název cílového kanálu IBM MQ na vzdálený systém.

Je-li tento atribut nastaven na hodnotu HOSTNAME, klienti s podporou SNI nastaví záhlaví SNI na název hostitele, což způsobí, že požadavky na odchozí připojení obdrží výchozí certifikát vzdáleného správce front během navázání komunikace TLS, a proto nelze použít certifikáty pro jednotlivé kanály.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Javaa IBM MQ classes for JMS .

Hodnoty vlastností jsou klientem Java/JMS interpretovány s rozlišováním velkých a malých písmen, takže hodnoty YES/NO by měly být nastaveny velkými písmeny.

V produktu IBM MQ 9.3.0byl IBM MQ spravovaný .NET klient aktualizován tak, aby nastavil NÁZEV SERVERU na příslušný název hostitele, pokud je vlastnost **OutboundSNI** nastavena na NÁZEV_HOSTITELE, což umožňuje klientovi IBM MQ spravovanému .NET připojení ke správci front pomocí Red Hat OpenShift tras.

Poznámka: Pokud se aplikace s nastavením **OutboundSNI** na hodnotu HOSTNAME připojí ke kanálu s nakonfigurovaným popiskem certifikátu, aplikace se odmítne s hodnotou MQRC_SSL_INITIALIZATION_ERROR a v protokolech chyb správce front se zobrazí zpráva AMQ9673 .

AllowOutboundSNI = YES (výchozí) | NE

Je-li tato volba povolena, klienti s podporou SNI nastaví SNI na název cílového kanálu IBM MQ pro vzdálený systém při inicializaci připojení TLS. Je-li tento atribut nastaven na hodnotu NO, klienti s podporou SNI nenastaví záhlaví SNI, což způsobí, že požadavky na odchozí připojení obdrží výchozí certifikát vzdáleného správce front během navázání komunikace TLS, a proto nelze použít certifikáty pro jednotlivé kanály.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Javaa IBM MQ classes for JMS .

Hodnoty vlastností jsou klientem Java/JMS interpretovány s rozlišováním velkých a malých písmen, takže hodnoty YES/NO by měly být nastaveny velkými písmeny.

Upozornění: Deprecated V 9.3.0 From IBM MQ 9.3.0 the **AllowOutboundSNI** property is deprecated, and is available for backwards-compatibility purposes only.

AllowOutboundSNI set to YES poskytuje stejnou funkci jako **OutboundSNI** nastavenou na CHANNEL, zatímco **AllowOutboundSNI** nastavenou na NO poskytuje stejnou funkci jako **OutboundSNI** nastavenou na HOSTNAME.

Pokud jsou v sekci SSL přítomny atributy **AllowOutboundSNI** i **OutboundSNI** , má přednost nastavení **OutboundSNI** .

IBM i ALW **AllowTLSV13 =Y | YES | T | TRUE (výchozí) | N | NO | F | FALSE**

Určuje, zda může správce front používat specifikace TLS 1.3 CipherSpecs (viz Povolení CipherSpecs).

Tento atribut mohou číst klienti C/C + +.

Tento atribut může mít následující hodnoty:

- Y (výchozí), YES (výchozí), T (výchozí) nebo TRUE (výchozí): Povoluje protokol TLS 1.3 , který umožňuje správci front používat protokol TLS 1.3 CipherSpecs.
- N, NO, Fnebo FALSE: Zakáže protokol TLS 1.3, což znamená, že správce front nemůže používat protokol TLS 1.3 CipherSpecs.

Poznámka: Při použití klienta MQI je hodnota **AllowTLSV13** odvozena, pokud není explicitně uvedena v sekci SSL souboru “Sekce SSL konfiguračního souboru klienta” na stránce 179 používaného aplikací. Další informace naleznete v tématu IBM MQ Klient MQI a TLS 1.3.

CDPCheckExtensions = YES|NO (výchozí)

CDPCheckExtensions uvádí, zda se kanály TLS v tomto správci front pokusí zkontrolovat servery CDP, které jsou pojmenované v rozšířeních certifikátu CrlDistribution.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Tento atribut může mít následující hodnoty:

- YES (výchozí nastavení): Kanály TLS se pokusí zkontrolovat servery CDP a určit, zda je digitální certifikát odvolán.
- NO: Kanály TLS se nepokoušejí kontrolovat servery CDP. Tato hodnota je výchozí.

CertificateLabel = *řetězec*

Popisek certifikátu definice kanálu.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Další informace viz Označení certifikátu (CERTLABL) .

CertificateValPolicy = *řetězec*

Určuje typ použitého ověření platnosti certifikátu.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Tento atribut může mít následující hodnoty:

ANY
Použijte všechny zásady ověřování certifikátů podporované základní knihovnou zabezpečených soketů. Toto nastavení je výchozí.

RFC5280
Použijte pouze ověření platnosti certifikátu, které je v souladu se standardem RFC 5280.

ClientRevocationKontroly = POVINNÉ|VOLITELNÉ|ZAKÁZÁNO
Určuje, jak je konfigurována kontrola odvolání certifikátů, pokud volání připojení klienta používá kanál TLS. Viz také **OCSPAuthentication**.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Tento atribut může mít následující hodnoty:

REQUIRED (výchozí)
Pokusí se načíst konfiguraci odvolání certifikátu z tabulky CCDT a provést kontrolu odvolání podle konfigurace. Pokud soubor CCDT nelze otevřít nebo není možné ověřit certifikát (například z důvodu nedostupnosti serveru OCSP nebo CRL), volání MQCONN selže. Pokud tabulka CCDT neobsahuje žádnou konfiguraci odvolání, neprovede se žádná kontrola odvolání, která by však nezpůsobila selhání kanálu.

Windows Na systémech Windows můžete také použít Active Directory pro kontrolu odvolání CRL. Pro kontrolu odvolání protokolu OCSP nelze použít službu Active Directory .

Pokud používáte MQSCO nebo CCDT, bude připojení úspěšné. Není-li k dispozici žádný soubor CCDT a není-li také zadán příkaz MQSCO, dojde k selhání připojení s kódem příčiny 2059 a protokol chyb hlásí `AMQ9518E: Soubor '/var/mqm/AMQCLCHL.TAB' nenalezeno.`

Volitelný
Co se týče volby `REQUIRED`, pokud však není možné načíst konfiguraci odvolání certifikátu, kanál neselže.

VYPNUTO
Nebyl proveden žádný pokus o načtení konfigurace odvolání certifikátu z tabulky CCDT a nebyla provedena žádná kontrola odvolání certifikátu.

Poznámka: Používáte-li spíše MQCONNX než volání MQCONN, můžete zvolit dodání záznamů ověřovacích informací (MQAIR) prostřednictvím MQSCO. Výchozí chování s MQCONNX proto neselhává, pokud soubor CCDT nelze otevřít, ale pokud předpokládáte, že dodáváte MQAIR (i když se rozhodnete tak neučinit).

EncryptionPolicySuiteB = *řetězec*
Určuje, zda kanál používá šifrování vyhovující standardu Suite-B a jakou úroveň síly má být použita.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Tento atribut může mít následující hodnoty:

NONE
Šifrování vyhovující standardu Suite-B se nepoužívá. Toto nastavení je výchozí.

128_BIT,192_BIT
Nastaví sílu zabezpečení na 128bitovou i 192bitovou úroveň.

128_BIT
Nastaví sílu zabezpečení na 128bitovou úroveň.

192_BIT
Nastaví sílu zabezpečení na 192bitovou úroveň.

V 9.3.0 ALW **EnvironmentScope=PROCESS|CONNECTION**
Řídí, zda produkt IBM MQ používá jediné prostředí IBM Global Security Kit (GSKit) pro celý proces nebo prostředí GSKit pro každé připojení.

Tento atribut mohou číst klienti jazyka C.

Tento atribut může mít následující hodnoty:

PROCESS
Jedno prostředí GSKit se používá pro více připojení vytvořených procesem. Použití tohoto nastavení znamená, že změny úložiště klíčů TLS nebudou k dispozici, dokud se nezastaví všechna aktivní připojení TLS v rámci procesu.

Tato hodnota je výchozí hodnota.

PŘIPOJENÍ
Pro každé připojení v rámci stejného procesu se vytvoří prostředí GSKit . Povolení této volby znamená, že změny úložiště klíčů TLS budou okamžitě vyzvednuty všemi novými připojeními TLS spuštěnými procesem.

Upozornění: Povolení tohoto provozního režimu způsobí, že aplikace budou používat další prostředky CPU a paměti k vytvoření každého prostředí GSKit . Tato spotřeba prostředků se zvyšuje s každým dalším souběžným připojením TLS.

ALW **MinimumRSAKeyvelikost=int**

Uvádí minimální velikost klíče, kterou musí mít certifikáty RSA, aby mohly být přijaty. Povoluje jakoukoli hodnotu rovnající se 0 nebo vyšší. Není-li uvedeno, použije se výchozí hodnota 1.

Tento atribut mohou číst klienti C/C + +.

OCSPAuthentication = VOLITELNÉ|POVINNÉ|VAROVÁNÍ
Definuje chování produktu IBM MQ , když je povolen protokol OCSP a kontrola odvolání protokolu OCSP nemůže určit stav odvolání certifikátu. Viz také **ClientRevocationChecks**.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Tento atribut může mít následující hodnoty:

Volitelný
Jakýkoli certifikát se stavem odvolání, který nelze určit kontrolou OCSP, je přijat a není generována žádná varovná ani chybová zpráva. Připojení SSL nebo TLS pokračuje, jako by nebyla provedena žádná kontrola odvolání.

POVINNÉ
Kontrola OCSP musí přinést konečný výsledek odvolání pro každý certifikát SSL nebo TLS, který je kontrolován. Jakýkoli 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 ReasonQualifier hodnoty MQRQ_SSL_HANDSHAKE_ERROR. Připojení je zavřeno.

Tato hodnota je výchozí hodnota.

WARN
Pokud se při kontrole odvolání protokolu OCSP nepodaří zjistit stav odvolání jakéhokoli certifikátu SSL nebo TLS, bude v protokolech chyb správce front ohlášeno varování. Jsou-li povoleny zprávy událostí SSL správce front, vygeneruje se zpráva MQRC_CHANNEL_SSL_VAROVÁNÍ s parametrem ReasonQualifier parametru MQRQ_SSL_UNKNOWN_REVOCATION. Připojení může pokračovat.

OCSPCheckExtensions = YES|NO
Řídí, zda produkt IBM MQ pracuje s rozšířeními certifikátu AuthorityInfoAccess.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

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

ALW **OCSPTimeout = *číslo***
Počet sekund čekání na odpovídací modul OCSP při provádění kontroly odvolání.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Pokud je v systému IBM MQ 9.3.0nastavena hodnota 0, použije se výchozí časový limit 30 sekund.

Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 30 sekund.

ALW **PeerCertChainValidation=*řetězec***

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Řetězec může mít jednu ze dvou hodnot:

- `Usepeerchain` **[výchozí]**: Řetěz certifikátů poskytnutý rovnocenným partnerem lze použít k překlenutí případných mezer v řetězu důvěryhodnosti při ověřování certifikátů. S výjimkou kořenového certifikátu.
- `Pouze úložiště údajů o důvěryhodnosti` **[Nedoporučeno]**: Pro ověření certifikátu partnera budou použity pouze certifikáty v úložišti údajů o důvěryhodnosti.

SSLCryptoHardware = *řetězec*

Nastaví řetězec parametrů nezbytný pro konfiguraci šifrovacího hardwaru PKCS #11 přítomného v systému.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Zadejte řetězec v následujícím formátu: `GSK_PKCS11 = driver path and filename;token label;token password;symmetric cipher setting;`

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 název souboru a cestu k ovladači PKCS #11 je `/usr/lib/pkcs11/PKCS11_API.so`. Chcete-li přistupovat k operacím symetrické šifry prostřednictvím produktu GSKit, zadejte parametr nastavení symetrické šifry. Hodnota tohoto parametru je buď:

SYMETRICKÝ_CIPHER_OFF
Nepřistupovat k operacím symetrické šifry. Toto nastavení je výchozí.

SYMETRICKÝ_CIPHER_ON
Přístup k operacím symetrické šifry.

Linux AIX Při zadávání různých komponent řetězce musíte změnit význam znaků středníku pomocí zpětného lomítka, protože znak středníku je považován za komentář. Například: `'\;'`

V 9.3.0 Měli byste chránit heslo tokenu obsažené v řetězci atributu **`SSLCryptoHardware`** . Další informace naleznete v tématu IBM MQ klienti používající šifrovací hardware .

V 9.3.0 Pro zpracování šifrovaných hesel nyní neexistuje žádné omezení délky řetězce.

Výchozí hodnota je prázdná. Pokud uvedete řetězec, který není ve správném formátu, vygeneruje se chyba.

SSLCryptoHardwareKeyFile = *pathname*

Úplná cesta a název souboru obsahujícího počáteční klíč, který byl použit k zašifrování hesla v řetězci konfigurace šifrovacího hardwaru PKCS #11 , který je uveden s atributem **`SSLCryptoHardware`** . Počáteční klíč musí být uveden, pokud byl uveden počáteční soubor s klíči, když bylo heslo v řetězci konfigurace šifrovacího hardwaru zašifrováno pomocí příkazu **`runp11cred`** . Další informace viz IBM MQ klienti používající kryptografický hardware.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

SSLFipsRequired = YES|NO

Uvádí, zda se mají použít pouze algoritmy certifikované FIPS, pokud se šifrování provádí v produktu IBM MQ.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Je-li konfigurován kryptografický hardware, používají se kryptografické moduly, které jsou poskytovány hardwarovým produktem. Ty mohou nebo nemusí být certifikovány FIPS na konkrétní úroveň, v závislosti na používaném hardwarovém produktu.

SSLHTTPProxyName = *řetězec*
Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má produkt GSKit použít pro kontroly OCSP. Za touto adresou může následovat volitelné číslo portu uzavřené v závorkách. Pokud číslo portu neurčíte, zvolí se výchozí port HTTP, který má číslo 80.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

AIX Pro 32bitové klienty na systému AIXmůže být síťová adresa pouze adresou IPv4 .

Na jiných platformách může být síťová adresa IPv4 nebo IPv6 .

Tento atribut může být nezbytný například v případě, že brána firewall zabraňuje přístupu k adrese URL odpovídacího modulu OCSP.

ALW **SSLHTTPConnectTimeout = *číslo*|0**
Počet sekund čekání na úspěšné vytvoření síťového připojení k serveru HTTP při provádění kontroly odvolání.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 0 (vypnuto).

SSLKeyRepository = *pathname*
V 9.3.0 V 9.3.0 Úplná cesta a název souboru úložiště klíčů, které obsahuje digitální certifikát uživatele. Pokud není uvedena přípona souboru, předpokládá se, že je `.kdb`.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

V 9.3.0 V 9.3.0 **SSLKeyRepositoryPassword = *passphrase***
Přístupová fráze pro přístup k úložišti klíčů. Hodnota může být řetězec prostého textu nebo přístupová fráze, která byla zašifrována pomocí obslužného programu **`runmqicred`** .

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

SSLKeyResetPočet = *integer*|0
Počet nešifrovaných bajtů odeslaných a přijatých kanálem TLS, než bude znovu vyjednán tajný klíč.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Hodnota musí být v rozsahu 0-999999999.

Výchozí hodnota je 0, což znamená, že tajné klíče nejsou nikdy znovu vyjednány.

Zadáte-li hodnotu 1-32768, budou kanály TLS používat počet resetů tajného klíče 32768 (32Kb). Tím se vyvarujte nadměrných resetů klíčů, které by se vyskytovaly pro malé hodnoty resetu tajného klíče.

Multi Sekce TCP konfiguračního souboru klienta

Použijte sekci TCP k uvedení konfiguračních parametrů síťového protokolu TCP.

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

Následující atributy lze zahrnout do sekce TCP:

ClntRcvBuffSize = *číslo*|0
Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech, kterou používá klientský konec kanálu připojení serveru pro připojení klienta.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávacích pamětí, na rozdíl od velikostí vyrovnávacích pamětí, které jsou opraveny produktem IBM MQ. Je-li hodnota nastavena

na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

CIntSndBuffSize = *číslo*|0
Velikost odesílací vyrovnávací paměti TCP/IP v bajtech, kterou používá klientský konec kanálu připojení serveru připojení klienta.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávacích pamětí, na rozdíl od velikostí vyrovnávacích pamětí, které jsou opraveny produktem IBM MQ. Je-li hodnota nastavena na nulu, použijí se předvolby operačního systému. Není-li nastavena žádná hodnota, použije se výchozí hodnota IBM MQ 32768.

Časový limit připojení = *number*
Počet sekund do vypršení časového limitu pokusu o připojení soketu.

Pokud **ConnectTimeout** = 0 a SOCK_NONBLOCK je vydán před asynchronním voláním connect (), volání není blokováno. Výchozí hodnota časového limitu 20 sekund (CONNECT_WAIT_MAX) je použitelná pro kontrolu stavu připojení.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Javaa IBM MQ classes for JMS .

Procesy kanálu IBM MQ se připojují přes neblokující sokety. Pokud tedy druhý konec soketu není připraven, funkce connect () se okamžitě vrátí s volbou *EINPROGRESS* nebo *EWOULDBLOCK*. Po tomto se neprovádí žádný pokus o opětovné připojení.

Je-li parametr Connect_Timeout nastaven na nenulovou hodnotu, produkt IBM MQ čeká na stanovené období volání select (), aby se soket dostal do stavu připravenosti. Tím se zvýší šance na úspěch následného volání connect (). Tato volba může být užitečná v situacích, kdy by připojení vyžadovala určitou čekací dobu kvůli vysokému zatížení sítě.

Mezi parametry Connect_Timeout, ClntSndBuffSizea ClntRcvBuffSize neexistuje žádný vztah.

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

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, spravovaní klienti .NETa spravovaní klienti XMS .NET .

Má možné hodnoty řetězce MQIPADDR_IPV4 nebo MQIPADDR_IPV6. Tyto hodnoty mají stejný význam jako IPV4 a IPV6 v produktu **ALTER QMGR IPADDRV** a proměnné prostředí **MQIPADDRV** .

KeepAlive = YES|NO
Zapněte nebo vypněte funkci KeepAlive . KeepAlive=YES způsobuje, že TCP/IP pravidelně kontroluje, zda je druhý konec připojení stále k dispozici. Pokud není, kanál se zavře.

Tento atribut mohou číst klienti C, nespravovaní klienti .NET, IBM MQ classes for Java, IBM MQ classes for JMS, spravovaní .NETa spravovaní klienti XMS .NET .

Windows **Library1 = *DLLName*|WSOCK32**
(pouze Windows) Název knihovny DLL soketů TCP/IP.

Tento atribut mohou číst klienti C a nespravovaní klienti .NET .

Windows V 9.3.3 Linux Trasovací sekce konfiguračního souboru klienta

Pomocí sekce Trasování povolte trasování pro knihovny klienta IBM MQ .NET a XMS .NET .

Následující atributy lze zahrnout do sekce TRACE:

MQDotnetTraceLevel=0 (výchozí) |1|2
Atribut **MQDotnetTraceLevel** se používá ke spuštění nebo zastavení trasování produktu IBM MQ .NET :

- 0: Zastaví trasování-toto je výchozí hodnota.
- 1: Spustí trasování s méně detaily.
- 2: Spustí trasování s úplnými podrobnostmi-doporučeno.

Tento atribut může číst spravovaný klient produktu IBM MQ .NET .

MQDotnetTracePath =*pathname*
Atribut **MQDotnetTracePath** ukazuje na složku, kde budou vytvořeny trasovací soubory produktu IBM MQ .NET . Aktuální adresář aplikace se použije, pokud je cesta prázdná nebo pokud není definována vlastnost **MQDotnetTracePath** .

Tento atribut může číst spravovaný klient produktu IBM MQ .NET .

MQDotnetErrorCesta =*název_cesty*
Atribut **MQDotnetErrorPath** ukazuje na složku, kde budou vytvořeny soubory protokolu chyb pro trasování produktu IBM MQ .NET . Aktuální adresář aplikace se použije, pokud je cesta prázdná nebo pokud není definován atribut **MQDonetErrorPath** .

Tento atribut může číst spravovaný klient produktu IBM MQ .NET .

XMSDotnetTraceLevel=0 (výchozí) |1|2
Atribut **XMSDotnetTraceLevel** se používá ke spuštění nebo zastavení trasování XMS .NET :

- 0: Zastaví trasování-toto je výchozí hodnota.
- 1: Spustí trasování se základním formátem.
- 2: Spustí trasování s rozšířeným formátem.

Tento atribut může číst spravovaný klient XMS .NET .

XMSDotnetTraceFilePath=*název_souboru*
Pokud není pro atribut **XMSDotnetTraceFilePath** nastavena hodnota, nebo pokud je tento atribut přítomen, ale obsahuje prázdný řetězec, je trasovací soubor pro XMS .NET umístěn do aktuálního adresáře. Chcete-li uložit trasovací soubor do pojmenovaného adresáře, zadejte název adresáře do adresáře **XMSDotnettraceFilePath**, například `XMSDotnetTraceFilePath="c:\somepath"`.

Tento atribut může číst spravovaný klient XMS .NET .

XMSDotnetTraceSpecification =*ComponentName=type=state*
Atribut **XMSDotnetTraceSpecification** uvádí název třídy, kterou chcete trasovat, a typ trasování, který požadujete pro XMS .NET:

- *ComponentName* je název třídy, kterou chcete trasovat. V tomto názvu můžete použít zástupný znak *. Například `*=all=enabled` uvádí, že chcete trasovat všechny třídy, a `IBM.XMS.impl.*=all=enabled` uvádí, že požadujete pouze trasování rozhraní API.
- *type* může být libovolný z následujících typů trasování: all, debug, event, EntryExit.
- *state* může být buď povoleno, nebo zakázáno.

Více prvků trasování můžete řetězit společně pomocí oddělovače ':' (dvojtečka).

Tento atribut může číst spravovaný klient XMS .NET .

XMSDotnetTraceFileSize=*velikost*
Atribut **XMSDotnetTraceFileSize** uvádí maximální velikost trasovacího souboru, který by měl být generován pro XMS .NET. Výchozí maximum je 20 MB, což je uvedeno jako `XMSDotnetTraceFileSize=20`.

Tento atribut může číst spravovaný klient XMS .NET .

XMSDotnetTraceFileNumber=*číslo*
Atribut **XMSDotnetTraceFileNumber** uvádí počet trasovacích souborů, které se mají uchovat pro XMS .NET. Výchozí hodnota je 4 (jeden aktivní soubor a tři archivní soubory). Minimální povolený počet je 2.

Tento atribut může číst spravovaný klient XMS .NET .

Související úlohy

Trasování IBM MQ aplikací .NET s mqclient.ini

Trasování aplikací XMS .NET pomocí souboru mqclient.ini

Multi Konfigurační soubor trasování aktivity mqat.ini

Konfigurační soubor trasování aktivity `mqat.ini`se používá ke konfiguraci chování trasování aktivity. Tento soubor se používá k definování úrovně a frekvence dat trasování aktivity vytváření sestav. Soubor také poskytuje způsob, jak definovat pravidla pro povolení a zakázání trasování aktivity na základě názvu aplikace.

Soubor `mqat.ini` následuje za stejným formátem dvojice klíč a hodnota parametru jako soubory `mqs.ini` a `qm.ini` . Soubor se skládá z jedné sekce, AllActivityTrace, která se standardně používá ke konfiguraci úrovně a frekvence vykazování dat trasování aktivity pro všechna trasování aktivity. Soubor může také obsahovat více sekcí ApplicationTrace . Každá z těchto sekcí definuje pravidlo pro chování trasování pro jedno nebo více připojení na základě shody názvu aplikace připojení k pravidlu. Další informace viz Trasování aktivity aplikace a Konfigurace chování trasování aktivity pomocí produktu `mqat.ini`.

Správce front používá řadu pravidel k určení, která nastavení sekcí se mají použít pro připojení. Volitelně můžete přepsat globální nastavení úrovně trasování a frekvence v sekci AllActivityTrasovací sekce pro ta připojení, která odpovídají sekci ApplicationTrace . Další informace naleznete v tématu Konfigurace chování trasování aktivity pomocí produktu `mqat.ini`.

Umístění adresářů

Linux IBM i AIX V systémech AIX and Linux a IBM i se soubor `mqat.ini` nachází v datovém adresáři správce front, což je stejné umístění jako soubor `qm.ini` .

Windows V systémech Windows se soubor `mqat.ini` nachází v datovém adresáři správce front `C:\Program Files\IBM\WebSphere MQ\qmgrs\queue_manager_name`. Uživatelé spouštějící aplikace, které mají být trasovány, potřebují oprávnění ke čtení tohoto souboru.

Multi AllActivitySekce trasování souboru mqat.ini

Sekce trasování AllActivitykonfiguračního souboru `mqat.ini` uvádí parametry, které se používají ke konfiguraci úrovní trasování pro správce front.

Jediná sekce trasování AllActivitydefinuje nastavení pro trasování aktivity, které se použije na všechna připojení produktu IBM MQ , pokud nejsou potlačena.

Jednotlivé hodnoty v sekci trasování AllActivitylze přepsat konkrétnějšími informacemi v sekci ApplicationTrace.

Je-li uveden více než jeden oddíl trasování AllActivity, použijí se hodnoty v poslední sekci. Parametry, které chybí ve zvoleném trasování AllActivity, mají výchozí hodnoty. Parametry a hodnoty z předchozích sekcí trasování AllActivityjsou ignorovány.

ActivityInterval
: Časový interval v sekundách mezi zprávami trasování. Trasování aktivity nepoužívá podproces časovače, takže zpráva trasování není zapsána přesně v okamžiku, kdy uplynula doba, je zapsána při provedení první operace MQI po uplynutí časového intervalu. Je-li tato hodnota 0, zpráva trasování se zapíše při odpojení připojení (nebo při dosažení počtu aktivit). Výchozí hodnota je 1.

ActivityCount
: Počet operací MQI mezi zprávami trasování. Pokud je tato hodnota 0, zpráva trasování se zapíše, když se připojení odpojí (nebo když uplyne interval aktivity). Výchozí hodnota je 100.

TraceLevel
Množství podrobností parametru, které jsou trasovány pro každou operaci. Popis podrobností jednotlivých operací, které parametry jsou zahrnuty pro každou úroveň trasování. Nastavte na hodnotu `LOW`, `MEDIUM`nebo `HIGH`. Výchozí hodnota je `MEDIUM`.

TraceMessageData
Množství dat zprávy trasovaných v bajtech pro operace MQGET, MQPUT, MQPUT1a Callback. Výchozí hodnota je 0.

StopOnGetTraceZpráva
Lze nastavit na hodnotu `ON` nebo `OFF`. Výchozí hodnota je `ON`.

SubscriptionDelivery
Lze nastavit na `BATCHED` nebo `IMMEDIATE`. Určuje, zda se mají použít parametry **`ActivityInterval`** a **`ActivityCount`** , když je přítomen jeden nebo více odběrů trasování aktivity. Nastavení tohoto parametru na hodnotu `IMMEDIATE` má za následek přepsání hodnot **`ActivityInterval`** a **`ActivityCount`** efektivními hodnotami 1 v případě, že data trasování mají odpovídající odběr. Každý záznam trasování aktivity není dávkován s jinými záznamy ze stejného připojení a místo toho je okamžitě doručen do odběru bez prodlevy. Nastavení `IMMEDIATE` zvyšuje režii výkonu při shromažďování dat trasování aktivity. Výchozí nastavení je `BATCHED`.

Související úlohy

Konfigurace chování trasování aktivity pomocí příkazu mqat.ini

Multi Sekce ApplicationTrace souboru mqat.ini

Konfigurační soubor `mqat.ini` může obsahovat více sekcí ApplicationTrace . Každá z těchto sekcí definuje pravidlo pro chování trasování pro jedno nebo více připojení na základě shody názvu aplikace připojení k pravidlu.

Pro sekci ApplicationTrace můžete nastavit následující hodnoty:

Trasovat
Přepínač trasování aktivity, který lze nastavit na hodnotu `ON` nebo `OFF`. Parametr **`Trace`** je povinný parametr bez výchozí hodnoty. Lze jej použít v sekci specifické pro aplikaci k určení, zda je trasování aktivity aktivní pro obor aktuální sekce aplikace. Všimněte si, že tato hodnota přepíše nastavení **`ACTVTRC`** a **`ACTVCONO`** pro správce front.

ApplName
Parametr **`ApplName`** je zadán jako znakový řetězec a jedná se o povinný parametr bez výchozí hodnoty. Tato hodnota se používá k určení aplikací, pro které se použije sekce ApplicationTrace . Shoduje se s hodnotou **`ApplName`** ze struktury kontextu uživatelské procedury rozhraní API (což je ekvivalent k produktu MQMD.PutApplName). Obsah hodnoty **`ApplName`** se liší v závislosti na prostředí aplikace.

Na platformě Multiplatforms se jedná pouze o část názvu souboru produktu MQAXC.ApplName se shoduje s hodnotou v sekci. Znaky nalevo od oddělovače cesty zcela vpravo jsou při porovnávání ignorovány.

Jeden zástupný znak (*) lze použít na konci hodnoty **`ApplName`** , aby odpovídal libovolnému počtu znaků za tímto bodem. Pokud je hodnota **`ApplName`** nastavena na jeden zástupný znak (*), pak hodnota **`ApplName`** odpovídá všem aplikacím.

IBM i **ApplFunction**
Parametr **`ApplFunction`** je uveden jako řetězec znaků. Výchozí hodnota je *. Hodnota tohoto parametru se používá ke kvalifikaci aplikačních programů, pro které se použije sekce ApplicationTrace a hodnota **`ApplName`** .

Sekce je volitelná a je platná pouze pro správce front IBM i . Jeden zástupný znak (*) lze použít na konci hodnoty **`ApplName`** , aby odpovídal libovolnému počtu znaků. Například sekce ApplicationTrace určující **`ApplName`** = ** a **`ApplFunction`** = *AMQSPUT0* platí pro všechna vyvolání programu AMQSPUT0 z libovolné úlohy.

ApplClass
Parametr **ApplClass** definuje třídu aplikace a lze jej nastavit na následující hodnoty:

- UŽIVATEL
- MCA
- ALL (Toto je výchozí hodnota)

Vysvětlení, jak hodnoty **AppType** odpovídají připojením IBM MQ , viz Tabulka 3 v tématu Konfigurace chování trasování aktivity pomocí souboru mqat.ini.

Volitelně lze globální nastavení úrovně trasování a frekvence v sekci AllActivityTrace stanza přepsat pro ta připojení, která odpovídají sekci ApplicationTrace .

Následující parametry lze nastavit v sekci ApplicationTrace . Pokud nejsou nastaveny, hodnota se zdědí z nastavení sekce trasování AllActivity :

ActivityInterval
Časový interval v sekundách mezi zprávami trasování. Trasování aktivity nepoužívá podproces časovače, takže zpráva trasování není zapsána přesně v okamžiku, kdy uplynula doba, je zapsána při provedení první operace MQI po uplynutí časového intervalu. Je-li tato hodnota 0, zpráva trasování se zapíše při odpojení připojení (nebo při dosažení počtu aktivit). Výchozí hodnota je 1.

ActivityCount
Počet operací MQI mezi zprávami trasování. Pokud je tato hodnota 0, zpráva trasování se zapíše, když se připojení odpojí (nebo když uplyne interval aktivity). Výchozí hodnota je 100.

TraceLevel
Množství podrobností parametru, které jsou trasovány pro každou operaci. Popis podrobností jednotlivých operací, které parametry jsou zahrnuty pro každou úroveň trasování. Nastavte na hodnotu LOW, MEDIUMnebo HIGH. Výchozí hodnota je MEDIUM.

TraceMessageData
Množství dat zprávy trasovaných v bajtech pro operace MQGET, MQPUT, MQPUT1a Callback. Výchozí hodnota je 0.

StopOnGetTraceZpráva
Lze nastavit na hodnotu ON nebo OFF. Výchozí hodnota je ON.

Související úlohy
Konfigurace chování trasování aktivity pomocí příkazu mqat.ini

Konfigurace distribuovaných front

Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

Než začnete

Před přečtením této části je užitečné porozumět kanálům, frontám a dalším konceptům představeným v tématu Distribuované fronty a klastry.

Potřebujete-li připojit dva správce front, kteří se nacházejí v různých fyzických sítích, nebo potřebujete-li komunikovat prostřednictvím brány firewall, může použití produktu IBM MQ Internet Pass-Thru zjednodušit konfiguraci. Další informace naleznete v tématu IBM MQ Internet Pass-Thru.

Procedura

- Informace v následujících dílčích tématech použijte k připojení aplikací pomocí distribuovaných front:
  - “IBM MQ techniky distribuovaného řazení do front” na stránce 190
  - “Úvod do správy distribuovaných front” na stránce 209
  - “Jak odeslat zprávu jinému správci front” na stránce 212

- “Spouštění kanálů” na stránce 233
- “Bezpečnost zpráv” na stránce 231
- ALW “Monitorování a řízení kanálů na systému AIX, Linux, and Windows” na stránce 240
- IBM i “Monitorování a řízení kanálů na systému IBM i” na stránce 263

Související pojmy

“nastaveníIBM MQ for z/OS” na stránce 876
Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

Související úlohy

“Konfigurace připojení mezi klientem a serverem” na stránce 14
Chcete-li konfigurovat komunikační spojení mezi produktem IBM MQ MQI clients a servery, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

“Konfigurace klastru správců front” na stránce 284
Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

“Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83
Úpravou informací v konfiguračních souborech (`.ini`) můžete změnit chování produktu IBM MQ nebo jednotlivého správce front tak, aby vyhovoval potřebám vaší instalace. Můžete také změnit volby konfigurace pro IBM MQ MQI clients.

“Konfigurace správců front v systému z/OS” na stránce 871
Pomocí těchto pokynů můžete konfigurovat správce front v systému IBM MQ for z/OS.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 950
Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

IBM MQ techniky distribuovaného řazení do front

Dílčí témata v této části popisují techniky, které se používají při plánování kanálů. Tato dílčí témata popisují techniky, které vám pomohou naplánovat, jak spojit správce front dohromady a spravovat tok zpráv mezi aplikacemi.

Příklady plánování kanálů zpráv viz:

- ALW Příklad plánování kanálu zpráv pro AIX, Linux, and Windows
- IBM i Příklad plánování kanálu zpráv pro IBM i
- z/OS Příklad plánování kanálu zpráv pro z/OS
- z/OS Příklad plánování kanálu zpráv pro z/OS použití skupin sdílení front

Související pojmy

Kanály
Úvod do řazení zpráv do fronty
Distribuované řazení do front a klastry

Související úlohy

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

Související odkazy

Příklad informací o konfiguraci

řízení toku zpráv

Řízení toku zpráv je úloha, která zahrnuje nastavení a údržbu tras zpráv mezi správci front. Je důležité pro přenosové cesty, které procházejí mnoha správci front. Tato část popisuje způsob použití front, definic alias front a kanálů zpráv v systému k dosažení řízení toku zpráv.

Tok zpráv řídíte pomocí řady technik, které byly zavedeny v produktu “Konfigurace distribuovaných front” na stránce 189. Pokud je váš správce front v klastru, je tok zpráv řízen pomocí různých technik, jak je popsáno v tématu “řízení toku zpráv” na stránce 191. z/OS Pokud jsou vaši správci front ve skupině sdílení front a je povoleno řazení do front v rámci skupiny (IGQ), může být tok zpráv řízen agenty IGQ. Tito agenti jsou popsáni v tématu Řízení front mezi skupinami.

K dosažení řízení toku zpráv můžete použít následující objekty:

- Přenosové fronty
- Kanály zpráv
- Definice vzdálené fronty
- Definice aliasu správce front
- Definice aliasu fronty pro odpověď

Správce front a objekty front jsou popsány v tématu Typy objektů. Kanály zpráv jsou popsány v tématu Distribuované komponenty front. Následující techniky používají tyto objekty k vytvoření toků zpráv ve vašem systému:

- Vkládání zpráv do vzdálených front
- Směrování prostřednictvím konkrétních přenosových front
- Příjem zpráv
- Předávání zpráv prostřednictvím systému
- Oddělení toků zpráv
- Přepnutí toku zpráv do jiného cíle
- Vyřešení názvu fronty pro odpověď na název aliasu

Poznámka

Všechny koncepty popsané v této části jsou relevantní pro všechny uzly v síti a zahrnují odesílací a přijímací konce kanálů zpráv. Z tohoto důvodu je ve většině příkladů uveden pouze jeden uzel. Výjimkou je situace, kdy příklad vyžaduje explicitní spolupráci administrátora na druhém konci kanálu zpráv.

Před tím, než budete pokračovat v jednotlivých technikách, je užitečné provést rekapitulaci konceptů rozlišování názvů a tří způsobů použití definic vzdálených front. Viz Distribuované řazení do front a klastry.

Související pojmy

“Názvy front v záhlaví přenosu” na stránce 191
Názvy cílových front se pohybují se zprávou v záhlaví přenosu, dokud není dosažena cílová fronta.

“Jak vytvořit správce front a odpovědět na aliasy” na stránce 192
Toto téma vysvětluje tři způsoby, jak vytvořit definici vzdálené fronty.

Názvy front v záhlaví přenosu

Názvy cílových front se pohybují se zprávou v záhlaví přenosu, dokud není dosažena cílová fronta.

Název fronty používaný aplikací, název logické fronty, je správcem front převeden na název cílové fronty. Jinými slovy, název fyzické fronty. Tento název cílové fronty prochází se zprávou v samostatné datové oblasti, v záhlaví přenosu, dokud není dosažena cílová fronta. Hlavička přenosu se pak odizoluje.

Při vytváření paralelních servisních tříd změníte část správce front tohoto názvu fronty. Nezapomeňte vrátit název správce front na původní název po dosažení konce odklonu provozní třídy.

Jak vytvořit správce front a odpovědět na aliasy

Toto téma vysvětluje tři způsoby, jak vytvořit definici vzdálené fronty.

Objekt definice vzdálené fronty se používá třemi různými způsoby. Tabulka 16 na stránce 192 vysvětluje, jak definovat každý ze tří způsobů:

- Použití definice vzdálené fronty k předefinování názvu lokální fronty.

  Aplikace poskytuje při otevírání fronty pouze název fronty a tento název fronty je název definice vzdálené fronty.

  Definice vzdálené fronty obsahuje názvy cílové fronty a správce front. Volitelně může definice obsahovat název přenosové fronty, která se má použít. Není-li zadán žádný název přenosové fronty, použije správce front pro název přenosové fronty název správce front převzatý z definice vzdálené fronty. Pokud není 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.

  Aplikace nebo program kanálu poskytuje při otevírání fronty název fronty spolu s názvem vzdáleného správce front.

  Pokud jste zadali definici vzdálené fronty se stejným názvem jako název správce front a ponechali jste název fronty v definici prázdný, nahradí správce front název správce front v otevřeném volání názvem správce front v definici.

  Kromě toho může definice obsahovat název přenosové fronty, která se má použít. Není-li zadán žádný název přenosové fronty, správce front převezme název správce front převzatý z definice vzdálené fronty pro název přenosové fronty. Pokud není definována přenosová fronta s tímto názvem, ale je definována výchozí přenosová fronta, použije se výchozí přenosová fronta.
- Použití definice vzdálené fronty k předefinování názvu fronty pro odpověď.

  Pokaždé, když aplikace vloží zprávu do fronty, může poskytnout název fronty pro odpovědi na zprávy, ale s prázdným názvem správce front.

  Pokud zadáte definici vzdálené fronty se stejným názvem jako fronta pro odpověď, lokální správce front nahradí název fronty pro odpověď názvem fronty z vaší definice.

  V definici můžete zadat název správce front, nikoli však název přenosové fronty.

Tabulka 16. Tři způsoby použití objektu definice vzdálené fronty

Použití	**Název správce front**	**Název fronty**	**Jméno přenosové fronty**
1. Definice vzdálené fronty (při volání OPEN)			
Dodáváno ve volání	prázdný nebo lokální QM	(*) vyžadováno	nelze použít
Dodává se v definici	povinné	povinné	volitelné
2. Alias správce front (při volání OPEN)			
Dodáváno ve volání	(*) povinný a nikoli lokální QM	povinné	nelze použít
Dodává se v definici	povinné	prázdná	volitelné
3. Alias fronty pro odpověď (při volání PUT)			
Dodáváno ve volání	prázdná	(*) vyžadováno	nelze použít
Dodává se v definici	volitelné	volitelné	prázdná

Poznámka: (*) znamená, že tento název je název objektu definice

Formální popis naleznete v tématu Rozlišení názvu fronty.

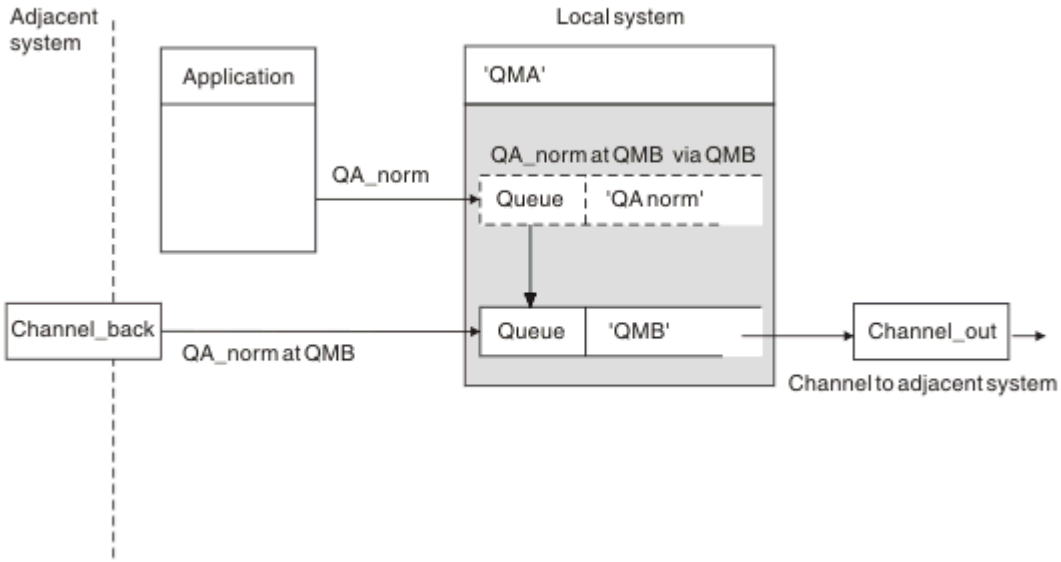
Vkládání zpráv do vzdálených front

Pomocí objektů definice vzdálené fronty lze převést název fronty na přenosovou frontu na sousedního správce front.

V prostředí s distribuovanými frontami jsou přenosová fronta a kanál ústředním bodem pro všechny zprávy v umístění bez ohledu na to, zda zprávy pocházejí z aplikací v lokálním systému, nebo zda přicházejí prostřednictvím kanálů ze sousedního systému. Obrázek 6 na stránce 193 zobrazuje aplikaci, která umísťuje zprávy do logické fronty s názvem 'QA_norm'. Rozlišení názvu používá definici vzdálené fronty 'QA_norm' k výběru přenosové fronty QMB. Poté přidá záhlaví přenosu do zpráv s označením 'QA_norm at QMB'.

Zprávy přicházející ze sousedního systému v 'Channel_back 'mají například záhlaví přenosu s názvem fyzické fronty' QA_norm at QMB '. Tyto zprávy jsou v přenosové frontě QMB umístěny beze změny.

Kanál přesune zprávy do sousedního správce front.



Obrázek 6. Definice vzdálené fronty se používá k rozlišení názvu fronty na přenosovou frontu na sousedního správce front.

Jste-li administrátorem systému IBM MQ , musíte:

- Definovat kanál zpráv ze sousedního systému
- Definovat kanál zpráv pro sousední systém
- Vytvořit přenosovou frontu QMB
- Definujte objekt vzdálené fronty 'QA_norm' pro překlad názvu fronty používaného aplikacemi na název cílové fronty, název správce cílové fronty a název přenosové fronty.

V klastrovaném prostředí je třeba definovat pouze přijímací kanál klastru v lokálním správci front. Nemusíte definovat přenosovou frontu nebo objekt vzdálené fronty. Viz Klastry.

Další informace o rozlišování názvů

Výsledkem definice vzdálené fronty je definování názvu fronty fyzického místa určení a názvu správce front. Tyto názvy jsou vloženy do záhlaví přenosu zpráv.

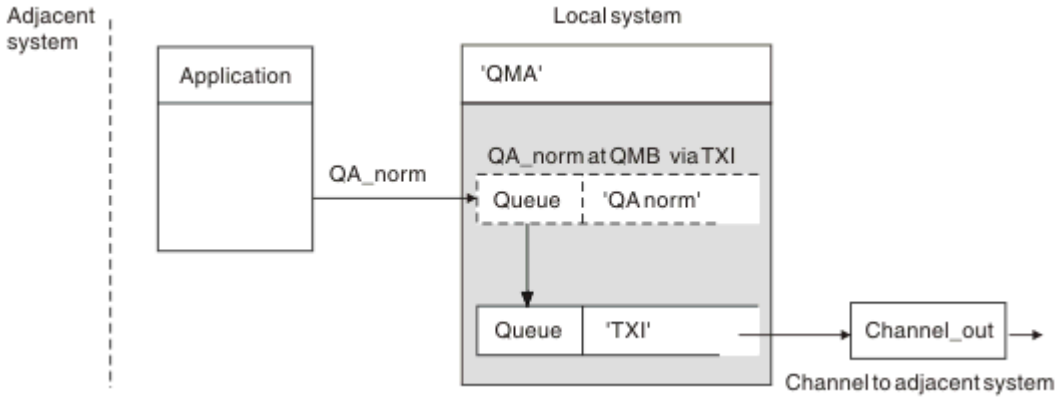
Příchozí zprávy ze sousedního systému již tento typ rozlišování názvů prováděly původní správce front. Proto mají záhlaví přenosu zobrazující název fyzické cílové fronty a název správce front. Tyto zprávy nejsou ovlivněny definicemi vzdálené fronty.

Související odkazy

Rozlišení názvu fronty

Výběr přenosové fronty

Pomocí definice vzdálené fronty můžete povolit jiné přenosové frontě odesílání zpráv stejnému sousednímu správci front.



Obrázek 7. Definice vzdálené fronty umožňuje použití jiné přenosové fronty

V prostředí s distribuovanými frontami platí, že pokud potřebujete změnit tok zpráv z jednoho kanálu na jiný, použijte stejnou konfiguraci systému, jak ukazuje Obrázek 6 na stránce 193 v části "Vkládání zpráv do vzdálených front" na stránce 193. Obrázek 7 na stránce 194 v tomto tématu ukazuje, jak používat definici vzdálené fronty k odesílání zpráv přes jinou přenosovou frontu, a tedy přes jiný kanál, do stejného sousedního správce front.

Pro konfiguraci zobrazenou v souboru Obrázek 7 na stránce 194musíte poskytnout objekt vzdálené fronty 'QA_norm' a přenosovou frontu 'TX1'. Musíte zadat 'QA_norm', abyste vybrali frontu 'QA_norm' ve vzdáleném správci front, přenosovou frontu 'TX1' a správce front 'QMB_priority'. Zadejte 'TX1' v definici kanálu sousedícího se systémem.

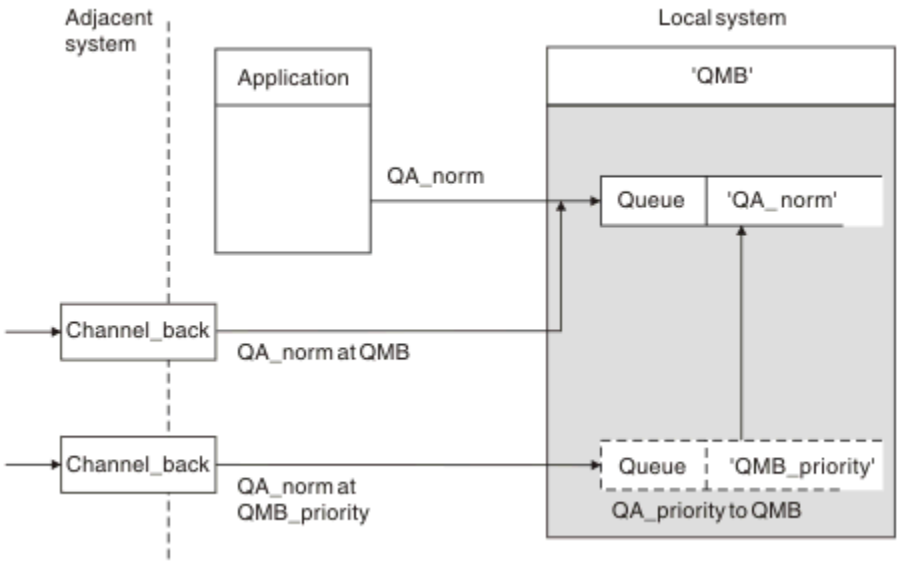
Zprávy jsou umístěny do přenosové fronty 'TX1' s přenosovým záhlavím obsahujícím 'QA_norm at QMB_priority' a jsou odesílány přes kanál do sousedního systému.

Kanál channel_back byl vynechán z tohoto obrázku, protože by vyžadoval alias správce front.

V klastrovaném prostředí nemusíte definovat přenosovou frontu nebo definici vzdálené fronty. Další informace viz "Definování front klastru" na stránce 285.

Příjem zpráv

Správce front můžete nakonfigurovat tak, aby přijímal zprávy od jiných správců front. Musíte se ujistit, že nedojde k neúmyslnému rozlišování názvů.



Obrázek 8. Příjem zpráv přímo a interpretace názvu správce front aliasu

Kromě uspořádání pro odesílání zpráv musí administrátor systému také zajistit, aby byly zprávy přijímány od sousedních správců front. Přijaté zprávy obsahují fyzický název cílového správce front a fronty v záhlaví přenosu. S nimi se zachází stejně jako se zprávami z lokální aplikace, která určuje název správce front i název fronty. Vzhledem k této léčbě je třeba zajistit, aby zprávy vstupující do vašeho systému neprováděly neúmyslné rozlišování jmen. Tento scénář naleznete v části Obrázek 8 na stránce 195 .

Pro tuto konfiguraci musíte připravit:

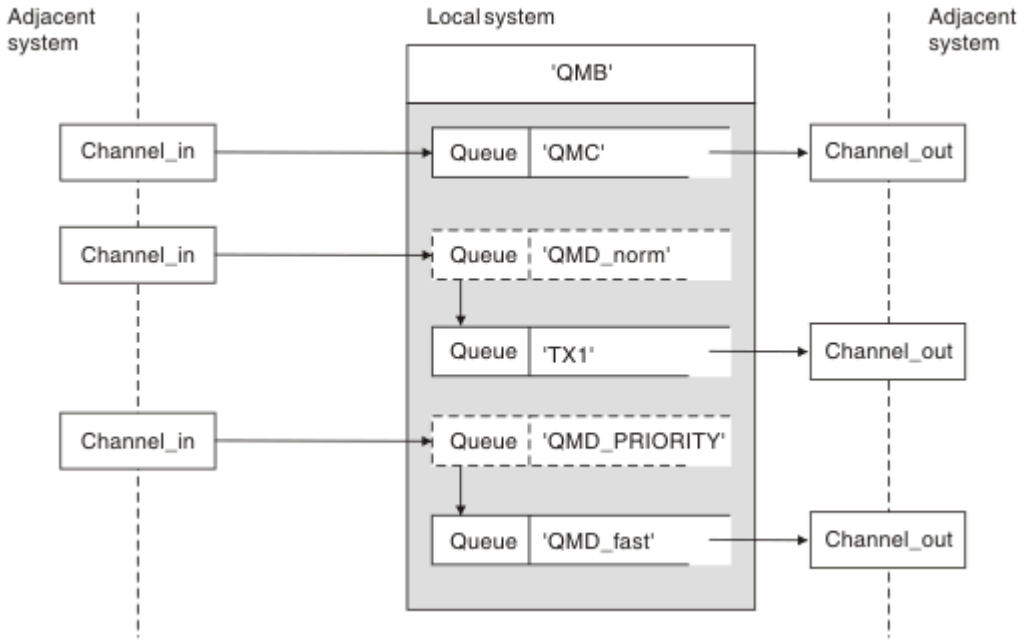
- Kanály zpráv pro příjem zpráv od sousedních správců front
- Definice aliasu správce front pro vyřešení příchozího toku zpráv 'QMB_priority' na název lokálního správce front 'QMB'
- Lokální fronta, 'QA_norm', pokud neexistuje

Názvy správců front s aliasem pro příjem

Použití definice aliasu správce front v tomto obrázku nevybralo jiného cílového správce front. Zprávy procházející tímto lokálním správcem front a adresované na 'QMB_priority' jsou určeny pro správce front 'QMB'. Alias názvu správce front se používá k vytvoření samostatného toku zpráv.

Předávání zpráv prostřednictvím systému

Zprávy můžete předávat prostřednictvím systému třemi způsoby-pomocí názvu umístění, pomocí aliasu pro správce front nebo výběrem přenosové fronty.



Obrázek 9. Tři metody předávání zpráv systémem

Technika zobrazená v souboru Obrázek 8 na stránce 195 v souboru “Příjem zpráv” na stránce 194ukázala, jak je zachycen tok aliasu. Obrázek 9 na stránce 196 ilustruje způsob, jakým jsou sítě vytvářeny, a to propojením dříve popsaných technik.

Konfigurace zobrazuje kanál doručující tři zprávy s různými cíli:

1. QB rovno QMC
2. QB rovno QMD_norm
3. QB rovno QMD_PRIORITY

Musíte projít prvním tokem zpráv v systému beze změny. Druhý tok zpráv musíte projít jinou přenosovou frontou a kanálem. Pro druhý tok zpráv musíte také vyřešit zprávy pro alias názvu správce front QMD_norm na správce front QMD. Třetí tok zpráv zvolí jinou přenosovou frontu bez jakékoli jiné změny.

V klastrovaném prostředí jsou zprávy předávány přes přenosovou frontu klastru. Obvykle jedna přenosová fronta SYSTEM.CLUSTER.TRANSMIT.QUEUEpřenáší všechny zprávy do všech správců front ve všech klastrech, jejichž je správce front členem. Viz Klastr správců front. Můžete definovat oddělené přenosové fronty pro všechny nebo některé správce front v klastrech, jejichž je správce front členem.

Následující metody popisují techniky použitelné pro prostředí distribuovaných front.

Použít tyto metody

Pro tyto konfigurace musíte připravit:

- Definice vstupního kanálu
- Definice výstupních kanálů
- Přenosové fronty:
  - QMC
  - TX1
  - QMD_fast
- Definice aliasů správce front:
  - QMD_norm s QMD_norm až QMD až TX1

– QMD_PRIORITY s QMD_PRIORITY až QMD_PRIORITY až QMD_fast

Poznámka: Žádný z toků zpráv zobrazených v příkladu nemění cílovou frontu. Aliasy názvů správců front zajišťují oddělení toků zpráv.

Metoda 1: Použít název příchozího umístění

Chystáte se přijímat zprávy se záhlavím přenosu obsahujícím jiný název umístění, například QMC. Nejjednodušší konfigurací je vytvořit přenosovou frontu s tímto názvem QMC. Kanál, který obsluňuje přenosovou frontu, doručí zprávu do dalšího místa určení beze změny.

Metoda 2: Použijte alias pro správce front

Druhou metodou je použití definice objektu aliasu správce front, ale určení nového názvu umístění QMDa konkrétní přenosové fronty TX1. Tato akce:

- Ukončí alias toku zpráv nastavený aliasem názvu správce front QMD_norm, tj. pojmenovanou provozní třídou QMD_norm.
- Změní záhlaví přenosu pro tyto zprávy z QMD_norm na QMD.

Metoda 3: Výběr přenosové fronty

Třetí metodou je, aby byl objekt aliasu správce front definován se stejným názvem jako cílové umístění QMD_PRIORITY. Pomocí definice aliasu správce front můžete vybrat konkrétní přenosovou frontu QMD_fast, a tedy jiný kanál. Záhlaví přenosu pro tyto zprávy zůstávají beze změny.

Oddělení toků zpráv

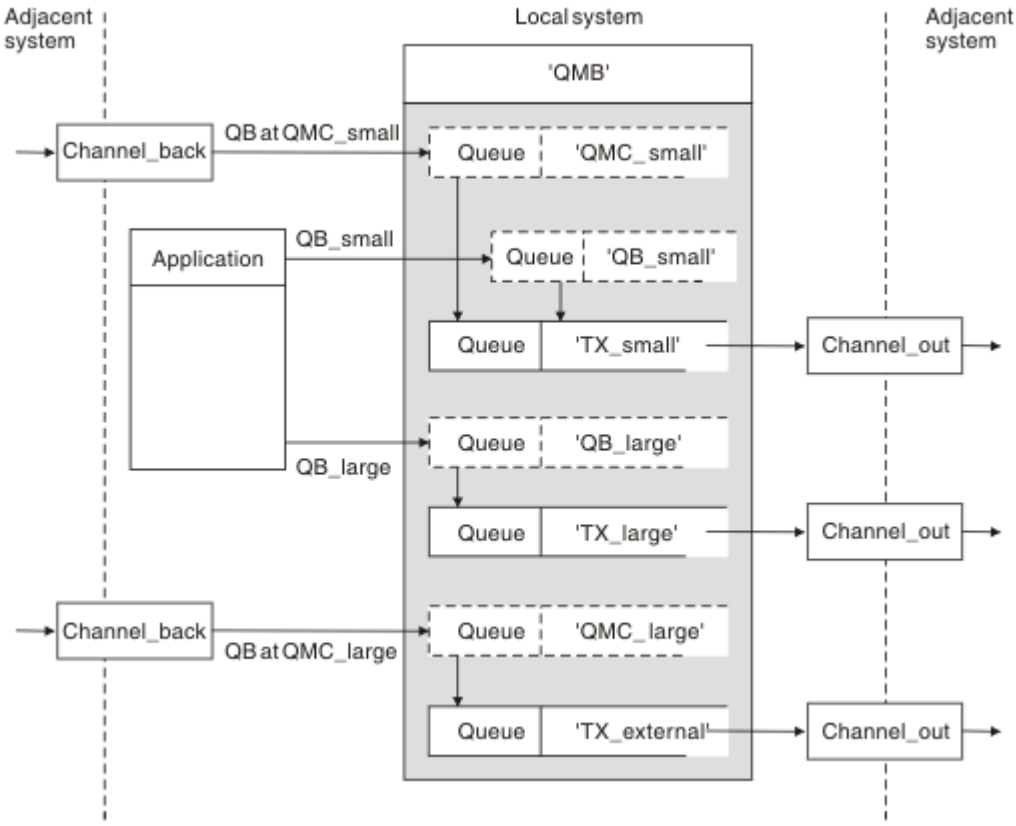
Alias správce front lze použít k vytvoření samostatných toků zpráv pro odesílání zpráv stejnému správci front.

Důvody pro rozdělení zpráv do různých toků zpráv

V prostředí s distribuovanými frontami může z mnoha příčin vzniknout potřeba oddělit zprávy pro stejného správce front do různých toků zpráv. Příklad:

- Možná budete muset poskytnout samostatný tok pro velké, střední a malé zprávy. Tato potřeba platí také v klastrovaném prostředí a v tomto případě můžete vytvořit klastry, které se překrývají. Existuje řada důvodů, proč tak můžete učinit, například:
  - Umožnit různým organizacím mít vlastní správu.
  - Umožnit samostatnou správu nezávislých aplikací.
  - Chcete-li vytvořit provozní třídu. Můžete mít například klastr s názvem STAFF, který je podmnožinou klastru s názvem STUDENTS. Když vložíte zprávu do fronty inzerované v klastru STAFF, použije se omezený kanál. Když vložíte zprávu do fronty inzerované v klastru STUDENTS, lze použít buď obecný kanál, nebo omezený kanál.
  - Chcete-li vytvořit testovací a produkční prostředí.
- Může být nezbytné směrovat příchozí zprávy různými cestami od 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 až do naplánování.

Příklad toku zpráv



Obrázek 10. Oddělení toků zpráv

V příkladu zobrazeném v souboru Obrázek 10 na stránce 198se jedná o dva příchozí toky s aliasem názvů správců front 'QMC_small' a 'QMC_large'. Těmto tokům poskytnete definici aliasu správce front pro zachycení těchto toků pro lokálního správce front. Máte aplikaci, která adresuje dvě vzdálené fronty, a tyto toky zpráv je třeba uchovávat odděleně. Zadáte dvě definice vzdálených front, které uvádějí stejné umístění, 'QMC', ale jiné přenosové fronty. Tato definice uchovává toky oddělené a na druhém konci není třeba nic dalšího, protože mají v záhlavích přenosu stejný název cílového správce front. Poskytujete:

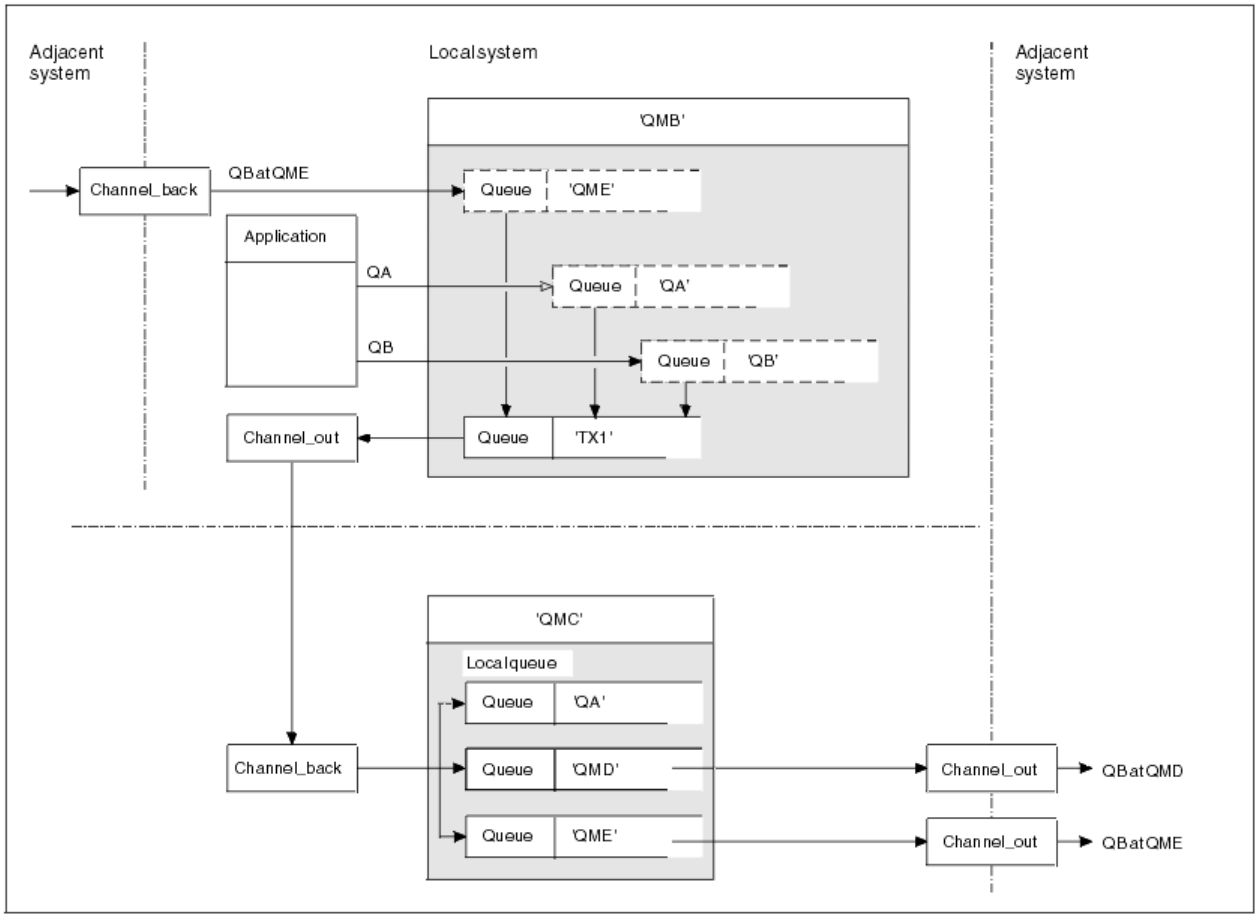
- Definice příchozích kanálů
- Dvě definice vzdálené fronty QB_small a QB_large
- Dvě definice aliasů správce front QMC_small a QMC_large
- Tři definice odesílajícího kanálu
- Tři přenosové fronty: TX_small, TX_large a TX_external

Koordinace se sousedními systémy

Použijete-li alias správce front k vytvoření samostatného toku zpráv, musíte tuto aktivitu koordinovat s administrátorem systému na vzdáleném konci kanálu zpráv, abyste se ujistili, že je zde k dispozici odpovídající alias správce front.

Soustředění zpráv do různých míst

Zprávy určené pro různá umístění můžete soustředit na jeden kanál.



Obrázek 11. Kombinování toků zpráv do kanálu

Obrázek 11 na stránce 199 ilustruje techniku distribuovaných front pro soustředění zpráv, které jsou určeny pro různá umístění na jednom kanálu. Dvě možná použití by byla:

- Soustředění přenosu zpráv prostřednictvím brány
- Použití širokých dálnic šířky pásma mezi uzly

V tomto příkladu jsou zprávy z různých zdrojů, lokální a sousední, které mají různé cílové fronty a správce front, přenášeny prostřednictvím přenosové fronty 'TX1' do správce front QMC. Správce front QMC doručí zprávy podle cílů. Jedna sada pro přenosovou frontu 'QMD' pro další přenos do správce front QMD. Další sada nastavená na přenosovou frontu 'QME' pro další přenos do správce front QME. Ostatní zprávy jsou vloženy do lokální fronty 'QA'.

Musíte poskytnout:

- Definice kanálů
- Přenosová fronta TX1
- Definice vzdálené fronty:
  - QA s 'QA v QMC přes TX1'
  - QB s 'QB na QMD přes TX1'
- Definice aliasu správce front:
  - QME s 'QME přes TX1'

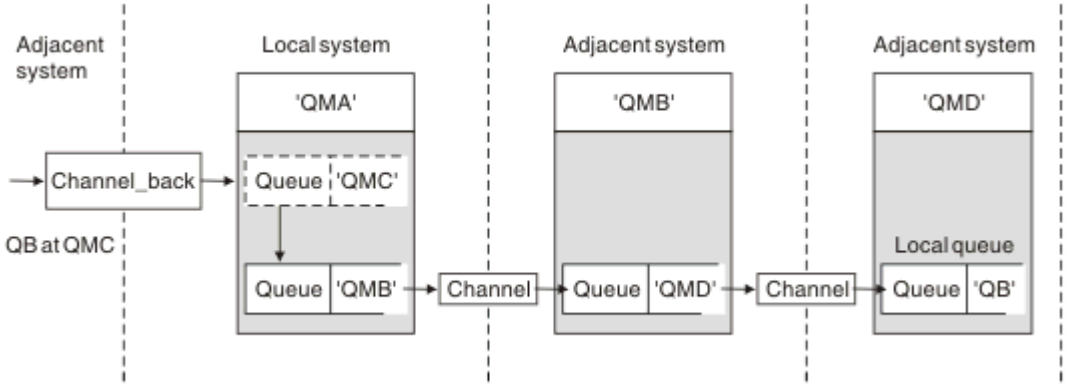
Doplňkový administrátor, který konfiguruje QMC, musí poskytnout:

- Definice přijímacího 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.

Přesměrování toků zpráv do jiného místa určení

Můžete předefinovat místo určení určitých zpráv pomocí aliasů správce front a přenosových front.



Obrázek 12. Přesměrování proudů zpráv do jiného místa určení

Obrázek 12 na stránce 200 ukazuje, jak můžete předefinovat cíl určitých zpráv. Příchozí zprávy do QMA jsou určeny pro 'QB at QMC'. Obvykle dorazí na QMA a jsou umístěny do přenosové fronty s názvem QMC, která byla součástí kanálu QMC. QMA musí přesměrovat zprávy na QMD, ale je schopen dosáhnout QMD pouze přes QMB. Tato metoda je užitečná, když potřebujete přesunout službu z jednoho místa na jiné a umožnit odběratelům pokračovat v odesílání zpráv dočasně, dokud se neupraví na novou adresu.

Metoda přesměrování příchozích zpráv určených pro určitého správce front na jiného správce front používá:

- Alias správce front pro změnu cílového správce front na jiného správce front a pro výběr přenosové fronty do sousedního systému.
- Přenosová fronta pro obsluhu sousedního správce front
- Přenosová fronta v sousedním správci front pro další směrování na cílového správce front.

Musíte poskytnout:

- Definice zpětného kanálu
- Definice objektu aliasu správce front QMC s QB v QMD až QMB
- Definice kanálu_ven
- Přidružená přenosová fronta QMB

Doplňkový administrátor, který konfiguruje QMB, musí poskytnout:

- Odpovídající definice channel_back
- Přenosová fronta, QMD
- Přidružená definice kanálu k QMD

Aliasy můžete použít v klastrovaném prostředí. Další informace viz “Aliasy a klastry správce front” na stránce 377.

Odesílání zpráv do distribučního seznamu

Můžete použít jedno volání MQPUT, aby aplikace odeslala zprávu do několika míst určení.

V produktu IBM MQ na všech platformách kromě platformy z/OSmůže aplikace odeslat zprávu do několika míst určení pomocí jediného volání MQPUT. Můžete tak učinit jak v prostředí s distribuovanými frontami,

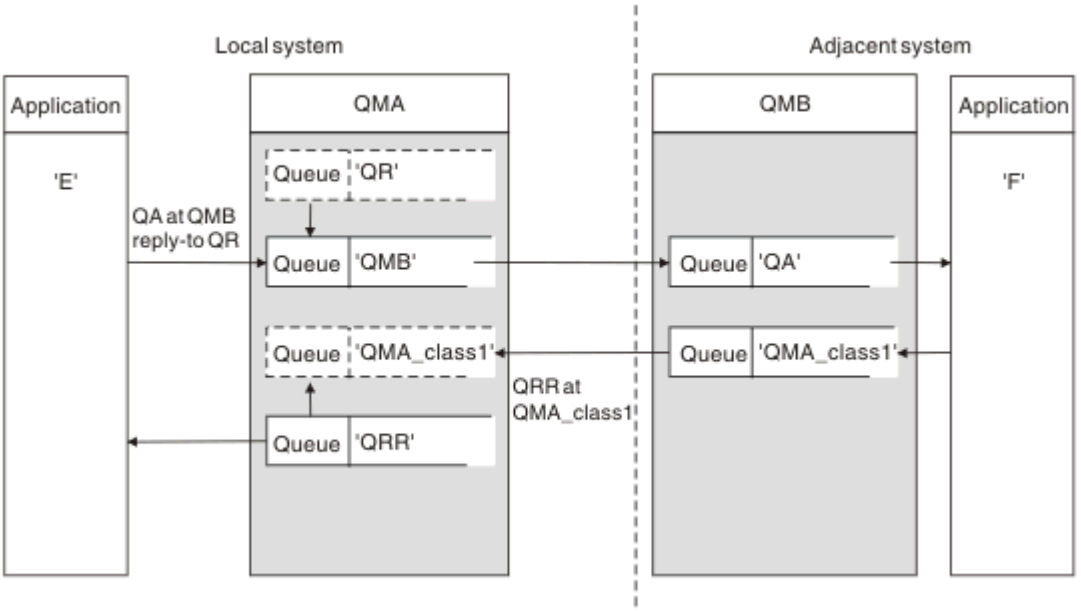
tak v klastrovaném prostředí. Musíte definovat cíle v distribučním seznamu, jak je popsáno v části Distribuční seznamy.

Ne všichni správci front podporují distribuční seznamy. Když agent MCA naváže spojení s partnerem, určí, zda partner podporuje distribuční seznamy, a příslušným způsobem nastaví příznak v přenosové frontě. Pokud se aplikace pokusí odeslat zprávu, která je určena pro distribuční seznam, ale partner nepodporuje distribuční seznamy, odesílající MCA zachytí zprávu a vloží ji do přenosové fronty jednou pro každý zamýšlený cíl.

Přijímající agent MCA zajišťuje, že zprávy odeslané do distribučního seznamu jsou bezpečně přijímány ve všech zamýšlených cílech. Pokud některá místa určení selžou, agent MCA určí, která z nich selhala. Poté pro ně může generovat sestavy výjimek a může se pokusit odeslat jim zprávy znovu.

Fronta pro odpověď

Můžete vytvořit úplnou vzdálenou smyčku zpracování fronty pomocí fronty pro odpověď.



Obrázek 13. Náhrada názvu fronty pro odpověď během volání PUT

Úplná smyčka zpracování vzdálené fronty používající frontu pro odpověď je zobrazena v části Obrázek 13 na stránce 201. Tato smyčka se používá jak v prostředí s distribuovanými frontami, tak v klastrovaném prostředí. Podrobnosti jsou uvedeny v části Tabulka 20 na stránce 208.

Aplikace otevře QA v QMB a vloží zprávy do této fronty. Zprávám je zadán název fronty pro odpověď QR, aniž by byl zadán název správce front. Správce front QMA vyhledá objekt fronty pro odpověď QR a extrahuje z něj název aliasu QRR a název správce front QMA_class1. Tyto názvy jsou vloženy do polí odpovědi na zprávy.

Zprávy odpovědí z aplikací v QMB jsou adresovány QRR na QMA_class1. Definici názvu aliasu správce front QMA_class1 používá správce front k toku zpráv do sebe a do fronty QRR.

Tento scénář znázorňuje způsob, jakým dáte aplikacím možnost zvolit provozní třídu pro zprávy s odpovědí. Třída je implementována přenosovou frontou QMA_class1 v QMB spolu s definicí aliasu správce front QMA_class1 v QMA. Tímto způsobem můžete změnit frontu pro odpověď aplikace tak, aby byly toky odděleny bez zapojení aplikace. Aplikace vždy zvolí QR pro tuto konkrétní provozní třídu. Máte možnost změnit provozní třídu s definicí QR fronty pro odpověď.

Musíte vytvořit:

- Definice fronty pro odpověď QR
- Objekt přenosové fronty QMB

- Definice kanálu_ven
- Definice zpětného kanálu
- Definice aliasu správce front QMA_class1
- Lokální objekt fronty QRR, pokud neexistuje

Doplňkový správce sousedního systému musí vytvořit:

- Definice přijímacího kanálu
- Objekt přenosové fronty QMA_class1
- Přidružený odesílající kanál
- Lokální objekt fronty QA.

Vaše aplikační programy používají:

- Název fronty pro odpověď QR ve volání vložení
- Název fronty QRR ve volání get

Tímto způsobem můžete změnit provozní třídu podle potřeby bez zapojení aplikace. Změníte alias odpovědi 'QR' spolu s přenosovou frontou 'QMA_class1' a aliasem správce front 'QMA_class1'.

Není-li při vkládání zprávy do fronty nalezen žádný objekt aliasu odpovědi, bude název lokálního správce front vložen do prázdného pole názvu správce front pro odpovědi. Název fronty pro odpověď zůstává nezměněn.

Omezení rozlišení názvů

Vzhledem k tomu, že při vložení původní zprávy bylo provedeno rozlišení názvu pro frontu pro odpověď na 'QMA', není v 'QMB ' povoleno žádné další rozlišení názvu. Zpráva je vložena odpovídající aplikací s fyzickým názvem fronty pro odpověď.

Aplikace si musí být vědomy toho, že název, který používají pro frontu pro odpovědi, se liší od názvu skutečné fronty, kde mají být nalezeny návratové zprávy.

Jsou-li například poskytnuty dvě provozní třídy pro použití aplikací s aliasem front pro odpovědi 'C1_alias' a 'C2_alias', aplikace používají tyto názvy jako názvy front pro odpovědi ve voláních vložení zpráv. Aplikace však ve skutečnosti očekávají, že se zprávy objeví ve frontách 'C1' pro 'C1_alias' a 'C2' pro 'C2_alias'.

Aplikace však může provést dotazové volání v alias frontě pro odpověď, aby sama zkontrolovala název skutečné fronty, kterou musí použít k získání zpráv odpovědi.

Související pojmy

“Jak vytvořit správce front a odpovědět na aliasy” na stránce 192
Toto téma vysvětluje tři způsoby, jak vytvořit definici vzdálené fronty.

“Příklad aliasu fronty pro odpověď” na stránce 202
Tento příklad ilustruje použití aliasu odpovědi pro výběr jiné přenosové cesty (přenosové fronty) pro vrácené zprávy. Použití tohoto prostředku vyžaduje změnu názvu fronty pro odpověď ve spolupráci s aplikacemi.

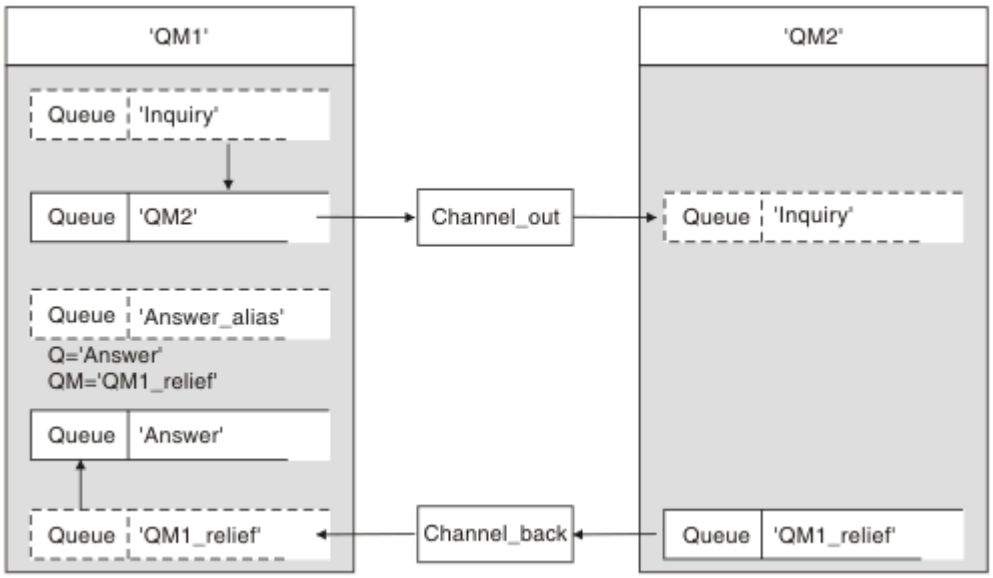
“Jak příklad funguje” na stránce 204
Vysvětlení příkladu a způsobu, jakým správce front používá alias fronty pro odpověď.

“Procházení aliasu fronty pro odpověď” na stránce 205
Průchod procesu z aplikace, která vkládá zprávu do vzdálené fronty, do stejné aplikace a odebírá zprávu odpovědi z alias fronty pro odpověď.

Příklad aliasu fronty pro odpověď

Tento příklad ilustruje použití aliasu odpovědi pro výběr jiné přenosové cesty (přenosové fronty) pro vrácené zprávy. Použití tohoto prostředku vyžaduje změnu názvu fronty pro odpověď ve spolupráci s aplikacemi.

Jak ukazuje Obrázek 14 na stránce 203, zpětná trasa musí být k dispozici pro zprávy odpovědí, včetně přenosové fronty, kanálu a aliasu správce front.



Obrázek 14. Příklad aliasu fronty pro odpověď

Tento příklad je určen pro aplikace žadatele na adrese 'QM1', které odesílají zprávy aplikacím serveru na adrese 'QM2'. Zprávy na serveru mají být vráceny prostřednictvím alternativního kanálu s použitím přenosové fronty 'QM1_relief' (výchozí návratový kanál by měl být 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', do pole pro odpověď všech zpráv, které vložily do fronty 'Dotaz'.

Definice fronty pro odpověď 'Answer_alias' je definována jako 'Odpověď na QM1_relief'. Aplikace v systému QM1 očekávají, že se jejich odpovědi objeví v lokální frontě s názvem 'Odpovědět'.

Serverové aplikace na adrese QM2 používají pole pro odpověď na přijaté zprávy k získání názvů front a správců front pro zprávy odpovědí pro žadatele na adrese QM1.

Definice použité v tomto příkladu na adrese QM1

Administrátor systému IBM MQ na adrese QM1 musí zajistit, aby byla fronta odpovědí 'Odpovědět' vytvořena spolu s ostatními objekty. Název aliasu správce front, označený znakem '*', musí odpovídat názvu správce front v definici aliasu fronty pro odpověď, který je také označen znakem '*'.

Objekt	**Definice**	
Lokální přenosová fronta	QM2	
Definice vzdálené fronty	Název objektu	Dotaz
	Název vzdáleného správce front	QM2
	Název vzdálené fronty	Dotaz
	Jméno přenosové fronty	QM2 (VÝCHOZÍ)
Alias správce front	Název objektu	QM1_relief *
	Název správce front	QM1
	Název fronty	(prázdné)
Alias fronty pro odpověď	Název objektu	Alias_odpovědi

Objekt	Definice	
	Název vzdáleného správce front	QM1_relief *
	Název vzdálené fronty	Odpověď

Vložit definici do QM1

Aplikace vyplní pole pro odpověď názvem aliasu fronty pro odpověď a ponechají pole názvu správce front prázdné.

Pole	Obsah
Název fronty	Dotaz
Název správce front	(prázdné)
Název fronty pro odpověď	Alias_odpovědi
Správce front pro odpovědi	(prázdné)

Definice použité v tomto příkladu na QM2

Administrátor systému IBM MQ na serveru QM2 se musí ujistit, že lokální fronta existuje pro příchozí zprávy a že správně pojmenovaná přenosová fronta je k dispozici pro zprávy odpovědi.

Objekt	Definice
Lokální fronta	Dotaz
Přenosová fronta	QM1_relief

Vložit definici na QM2

Aplikace na serveru QM2 načtou název fronty pro odpověď a název správce front z původní zprávy a použijí je při vkládání zprávy odpovědi do fronty pro odpověď.

Pole	Obsah
Název fronty	Odpověď
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 na adrese QM1 vždy používají 'Answer_alias' jako frontu pro odpověď v příslušném poli volání vložení. Vždy načítají své zprávy z fronty s názvem 'Odpovědět'.

Definice aliasů fronty pro odpověď jsou k dispozici pro použití administrátorem systému QM1 ke změně názvu fronty pro odpověď a návratové trasy 'QM1_relief'.

Změna názvu fronty 'Odpovědět' není obvykle užitečná, protože aplikace QM1 očekávají své odpovědi v této frontě. Avšak administrátor systému QM1 je schopen podle potřeby změnit cestu návratu (provozní třídu).

Způsob, jakým správce front používá alias fronty pro odpovědi

Správce front QM1 načte definice z aliasu fronty pro odpověď, pokud je název fronty pro odpověď zahrnutý ve volání vložení aplikací stejný jako alias fronty pro odpověď a část správce front je prázdná.

Správce front nahradí název fronty pro odpověď ve volání vložení názvem fronty z definice. Nahradí prázdný název správce front ve volání vložení názvem správce front z definice.

Tyto názvy jsou přenášeny se zprávou v deskriptoru zprávy.

Tabulka 17. Alias fronty pro odpověď		
Název pole	**Vložit volání**	**Záhlaví přenosu**
Název fronty pro odpověď	Alias_odpovědi	Odpověď
Název správce front pro odpověď	(prázdné)	QM1_relief

Procházení aliasu fronty pro odpověď

Průchod procesu z aplikace, která vkládá zprávu do vzdálené fronty, do stejné aplikace a odebírá zprávu odpovědi z alias fronty pro odpověď.

Pro dokončení tohoto příkladu se podívejme na proces.

1. Aplikace otevře frontu s názvem 'Dotaz' a vloží do ní zprávy. Aplikace nastaví pole pro odpověď 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 kontrolou definice vzdálené fronty s názvem 'Answer_alias'. Není-li žádný nalezen, umístí správce front svůj vlastní název 'QM1' do pole správce front pro odpověď deskriptoru zprávy.
3. Pokud správce front nalezne definici vzdálené fronty s názvem 'Answer_alias', extrahuje název fronty a názvy správců front z definice (queue name= 'Answer' a queue manager name= 'QM1_relief'). Pak je vloží do polí odpovědi na deskriptor zprávy.
4. Správce front 'QM1' používá definici vzdálené fronty 'Dotaz' k určení, že zamýšlená cílová fronta je ve správci front 'QM2' a že zpráva je umístěna 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 'Dotaz' a správce cílové fronty 'QM2'.
6. Zpráva dorazí do správce front 'QM2' a je umístěna do lokální fronty 'Inquiry'.
7. Aplikace získá zprávu z této fronty a zpracuje zprávu. Aplikace připraví zprávu odpovědi a vloží tuto zprávu odpovědi do názvu fronty pro odpověď z deskriptoru zprávy původní zprávy:

Název fronty pro odpověď	**Odpověď**
Název správce front pro odpověď	QM1_relief

8. Správce front 'QM2' provede příkaz put. Zjištění, že název správce front 'QM1_relief' je vzdálený správce front, umístí zprávu do přenosové fronty se stejným názvem 'QM1_relief'. Zprávě je poskytnuto záhlaví přenosu obsahující název cílové fronty 'Answer' a správce cílové fronty 'QM1_relief'.
9. Zpráva je přenesena do správce front 'QM1'. Správce front rozpoznává, že název správce front 'QM1_relief' je alias, extrahuje z definice aliasu 'QM1_relief' název fyzického správce front 'QM1'.
10. Správce front 'QM1' poté vloží zprávu do názvu fronty obsaženého v záhlaví přenosu 'Answer'.
11. Aplikace extrahuje zprávu odpovědi z fronty 'Answer'.

Aspekty sítě

V prostředí s distribuovanými frontami platí určitá pravidla, protože místa určení zpráv jsou adresována pouze s názvem fronty a názvem správce front.

1. Kde je zadán název správce front a název se liší od názvu lokálního správce front:
   - Přenosová fronta musí být k dispozici se stejným názvem. Tato přenosová fronta musí být součástí kanálu zpráv, který přesouvá zprávy do jiného správce front, nebo
   - Definice aliasu správce front musí existovat, aby bylo možné převést název správce front na stejný nebo jiný název správce front a volitelnou přenosovou frontu, nebo

- Pokud nelze název přenosové fronty interpretovat a byla definována výchozí přenosová fronta, použije se výchozí přenosová fronta.

2. V případě, že je zadán pouze název fronty, musí být v lokálním správci front k dispozici fronta libovolného typu, ale se stejným názvem. Tato fronta může být definicí vzdálené fronty, která se interpretuje jako: přenosová fronta na sousedního správce front, název správce front a volitelná přenosová fronta.

Chcete-li zjistit, jak to funguje v klastrovaném prostředí, prohlédněte si téma Klastry.

z/OS Pokud jsou správci front spuštěni ve skupině sdílení front (QSG) a je povoleno řazení do front v rámci skupiny (IGQ), můžete použít systém SYSTEM.QSG.TRANSMIT.QUEUE. Další informace naleznete v tématu Řízení front mezi skupinami.

Zvažte scénář, kdy kanál zpráv přesouvá zprávy z jednoho správce front do jiného v prostředí s distribuovanými frontami.

Přesouvané zprávy pocházejí z jiného správce front v síti a některé zprávy mohou být doručeny s neznámým názvem správce front jako místem určení. K tomuto problému může dojít například v případě, že se název správce front změnil nebo byl ze systému odebrán.

Program kanálu tuto situaci rozpozná, když nemůže najít přenosovou frontu pro tyto zprávy, a umístí zprávy do fronty nedoručených zpráv (nedoručených zpráv). Je na vás, abyste tyto zprávy vyhledali a zařídili jejich předání do správného místa určení. Případně je vraťte původci, u kterého lze původce zjistit.

Sestavy výjimek jsou generovány za těchto okolností, pokud byly zprávy sestavy vyžádány v původní zprávě.

Konvence rozlišení názvů

Rozlišování názvů, které mění identitu cílové fronty (tj. mění logický název na fyzický název), se vyskytuje pouze jednou a pouze v původním správci front.

Následné použití různých možností aliasu lze použít 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 distribuovaných front, tak v klastrovaném prostředí.

Tato adresa je obvykle určena aplikací, která zprávu vytváří. Může být upraven jakoukoli aplikací, která pak zpracuje zprávu, včetně aplikací uživatelských procedur.

Bez ohledu na zdroj této adresy se může každá aplikace, která zpracovává zprávu, rozhodnout, že použije tuto adresu pro vrácení odpovědi, stavu nebo zprávy sestavy do původní aplikace.

Způsob, jakým jsou tyto zprávy odpovědí směrovány, se neliší od způsobu, jakým je směrována původní zpráva. Je třeba si uvědomit, že toky zpráv, které vytvoříte pro jiné správce front, vyžadují odpovídající návratové toky.

Konflikty fyzických názvů

Název cílové fronty pro odpověď byl převeden na název fyzické fronty v původním správci front. V odpovídajícím správci front nesmí být znovu rozpoznán.

Jedná se o pravděpodobnou možnost problémů s konfliktem názvů, kterým lze zabránit pouze prostřednictvím síťové dohody o fyzických a logických názvech front.

Správa překladů názvů front

Při vytváření definice aliasu správce front nebo definice vzdálené fronty se rozlišování názvů provádí pro každou zprávu s tímto názvem. Tato situace musí být spravována.

Tento popis je poskytován návrhářům aplikací a plánovačům kanálů zabývajících se individuálním systémem, který má kanály zpráv pro sousední systémy. To trvá místní pohled na plánování a řízení kanálů.

Při vytváření definice aliasu správce front nebo definice vzdálené fronty se rozlišování názvů provádí pro každou zprávu nesoucí tento název bez ohledu na zdroj zprávy. Chcete-li dohlížet na tuto situaci, která může zahrnovat velký počet front v síti správců front, uchovávejte tabulky:

- Názvy zdrojových front a správců zdrojových front s ohledem na vyřešené názvy front, vyřešené názvy správců front a vyřešené názvy přenosových front s metodou rozpoznání
- Názvy zdrojových front s ohledem na:
  - Vyřešené názvy cílových front
  - Vyřešené názvy správců cílových front
  - Přenosové fronty
  - Názvy kanálů zpráv
  - Názvy sousedních systémů
  - Názvy front pro odpovědi

Poznámka: Použití výrazu *zdroj* v tomto kontextu odkazuje na název fronty nebo na název správce front poskytnutý aplikací nebo na program kanálu při otevírání fronty pro vkládání zpráv.

Příklad každé z těchto tabulek je uveden v tabulkách Tabulka 18 na stránce 207, Tabulka 19 na stránce 207a Tabulka 20 na stránce 208.

Názvy v těchto tabulkách jsou odvozeny z příkladů v této sekci a tato tabulka není určena jako praktický příklad rozlišení názvu fronty v jednom uzlu.

Tabulka 18. Rozlišení názvů front ve správci front QMA

Zdrojová fronta určená při otevření fronty	Zdrojový správce front zadaný při otevření fronty	Název vyřešené fronty	Vyřešený název správce front	Název vyřešené přenosové fronty	Typ rozlišení
QA_norm	-	QA_norm	QMB	QMB	Vzdálená fronta
(libovolná)	QMB	-	-	QMB	(není)
QA_norm	-	QA_norm	QMB	TX1	Vzdálená fronta
QB	QMC	QB	QMD	QMB	Alias správce front

Tabulka 19. Rozlišení názvů front ve správci front QMB

Zdrojová fronta určená při otevření fronty	Zdrojový správce front zadaný při otevření fronty	Název vyřešené fronty	Vyřešený název správce front	Název vyřešené 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
(libovolná)	QMC	(libovolná)	QMC	QMC	(není)
(libovolná)	QMD_norm	(libovolná)	QMD_norm	TX1	Alias správce front

Tabulka 19. Rozlišení názvů front ve správci front QMB (pokračování)					
Zdrojová fronta určená při otevření fronty	**Zdrojový správce front zadaný při otevření fronty**	**Název vyřešené fronty**	**Vyřešený název správce front**	**Název vyřešené přenosové fronty**	**Typ rozlišení**
(libovolná)	QMD_PRIORITY	(libovolná)	QMD_PRIORITY	Rychle_QMD_	Alias správce front
(libovolná)	QMC_small	(libovolná)	QMC_small	TX_malé	Alias správce front
(libovolná)	QMC_large	(libovolná)	QMC_large	TX_externí	Alias správce front
QB_small	QMC	QB_small	QMC	TX_malé	Vzdálená fronta
QB_large	QMC	QB_large	QMC	TX_large	Vzdálená fronta
(libovolná)	QME	(libovolná)	QME	TX1	Alias správce front
QA	QMC	QA	QMC	TX1	Vzdálená fronta
QB	QMD	QB	QMD	TX1	Vzdálená fronta

Tabulka 20. Překlad názvu fronty pro odpověď ve správci front QMA			
Návrh aplikací		**Definice aliasu pro odpověď**	
Lokální správce front	**Název fronty pro zprávy**	**Název aliasu fronty pro odpověď**	**Předefinováno na**
QMA	QRR	QR	QRR na QMA_class1

Pořadové číslo zprávy kanálu

Kanál používá pořadová čísla ke kontrole, zda jsou zprávy doručovány ve stejném pořadí, v jakém jsou převzaty z přenosové fronty.

Pořadová čísla kanálu jsou kontrolována při spuštění kanálu a v případě, že by došlo k neshodě, znamená to, že trvalá synchronizační data byla ztracena na obou stranách kanálu; například konfigurace zotavení z havárie (DR) nebo že ukončení dávkového zpracování bylo přerušeno, když byl kanál nejistý.

Resetování nebo ignorování neshod pořadových čísel, viz **IgnoreSeqNumberMismatch** v sekci *Kanály v souboru qm.ini*, nehrozí ztráta nebo duplikování dávky zpráv a neresetuje nejistý stav kanálu.

Tyto informace lze zobrazit pomocí volby DISPLAY CHSTATUS. Pořadové číslo a identifikátor s názvem LUWID jsou uloženy v trvalém úložišti pro poslední zprávu přenesenou v dávce. Tyto hodnoty se používají během spouštění kanálu, aby se zajistilo, že se oba konce odkazu dohodnou na tom, které zprávy byly úspěšně přeneseny.

Sekvenční načítání zpráv

Pokud aplikace vloží posloupnost zpráv do stejné cílové fronty, mohou být tyto zprávy načteny v posloupnosti pomocí aplikace ***single*** s posloupností operací MQGET, jsou-li splněny následující podmínky:

- Všechny požadavky vložení byly provedeny ze stejné aplikace.
- Všechny požadavky na vložení byly buď ze stejné pracovní jednotky, nebo byly všechny požadavky na vložení provedeny mimo pracovní jednotku.
- Všechny zprávy mají stejnou prioritu.
- Všechny zprávy mají stejnou perzistenci.

- V případě vzdáleného řazení do fronty je konfigurace taková, že může existovat pouze jedna cesta od aplikace, která vytváří požadavek na vložení, přes jejího správce front, přes interkomunikaci, do cílového správce front a do cílové fronty.
- Zprávy nejsou vloženy do fronty nedoručených zpráv (například pokud je fronta dočasně plná).
- Aplikace, která zprávu získává, záměrně nezmění pořadí načtení, například uvedením konkrétního *MsgId* nebo *CorrelId* nebo pomocí priorit zpráv.
- Pouze jedna aplikace provádí operace získání pro načtení zpráv z cílové fronty. Pokud existuje více než jedna aplikace, musí být tyto aplikace navrženy tak, aby získaly všechny zprávy v jednotlivých posloupnostech vložených odesílající aplikací.

Poznámka: Zprávy z jiných úloh a pracovních jednotek mohou být prokládány s posloupností, a to i v případě, že posloupnost byla vložena z jedné pracovní jednotky.

Pokud tyto podmínky nelze splnit a pořadí zpráv v cílové frontě je důležité, pak může být aplikace kódována tak, aby používala své vlastní pořadové číslo zprávy jako součást zprávy pro zajištění pořadí zpráv.

Posloupnost načítání rychlých přechodných zpráv

Přechodné zprávy na rychlém kanálu mohou předjíždět trvalé zprávy na stejném kanálu, a proto přicházejí mimo pořadí. Přijímající agent MCA okamžitě vloží přechodné zprávy do cílové fronty a zviditelní je. Trvalé zprávy nejsou viditelné až do dalšího synchronizačního bodu.

Testování zpětné smyčky

Testování zpětné smyčky je technika na platformách jiných než z/OS , která umožňuje testovat komunikační spojení bez skutečného propojení s jiným počítačem.

Nastavíte připojení mezi dvěma správci front, jako by byli umístěni na samostatných počítačích, ale připojení otestujete tak, že se vrátíte zpět do jiného procesu na stejném počítači. Tato technika znamená, že můžete testovat komunikační kód bez nutnosti aktivní sítě.

Způsob, jakým tak učiníte, závisí na tom, které produkty a protokoly používáte.

V systémech Windows můžete použít adaptér "loopback".

Další informace naleznete v dokumentaci k produktům, které používáte.

Trasování trasy a záznam aktivity

Trasu, kterou zpráva prochází řadou správců front, můžete potvrdit dvěma způsoby.

Můžete použít IBM MQ aplikaci zobrazení trasy, která je k dispozici prostřednictvím řídicího příkazu **dspmqrte**, nebo můžete použít záznam aktivity. Obě tato témata jsou popsána v části Odkaz na monitorování.

Úvod do správy distribuovaných front

Distribuovaná správa front (DQM) se používá k definování a řízení komunikace mezi správci front.

Správa distribuovaných front:

- Umožňuje definovat a řídit komunikační kanály mezi správci front.
- Poskytuje službu kanálu zpráv pro přesun zpráv z typu *lokální fronty*, známého jako přenosová fronta, do komunikačních spojení v lokálním systému a z komunikačních spojení do lokálních front v cílovém správci front.
- Poskytuje zařízení pro monitorování provozu kanálů a diagnostiku problémů pomocí panelů, příkazů a programů.

Definice kanálů přidružují názvy kanálů k přenosovým frontám, identifikátorům komunikačních spojů a atributům kanálů. Definice kanálů jsou implementovány různými způsoby na různých platformách.

Odesílání a příjem zpráv je řízen programy známými jako *agenti kanálu zpráv* (MCA), které používají definice kanálů ke spuštění a řízení komunikace.

Tyto MCA jsou následně řízeny samotným DQM. Struktura je závislá na platformě, ale obvykle zahrnuje moduly listener a monitory spouštěčů, spolu s příkazy operátora a panely.

Kanál zpráv je jednosměrné propojení procesů pro přesouvání zpráv z jednoho správce front do jiného. Kanál zpráv má tedy dva koncové body, které jsou reprezentovány dvojicí MCA. Každý koncový bod má definici svého konce kanálu zpráv. Například jeden konec by definoval odesílatele, druhý konec příjemce.

Podrobnosti o tom, jak definovat kanály, viz:

- ALW "Monitorování a řízení kanálů na systému AIX, Linux, and Windows" na stránce 240
- z/OS "Monitorování a řízení kanálů na systému z/OS" na stránce 954
- IBM i "Monitorování a řízení kanálů na systému IBM i" na stránce 263

Příklady plánování kanálů zpráv viz:

- ALW Příklad plánování kanálu zpráv pro AIX, Linux, and Windows
- IBM i Příklad plánování kanálu zpráv pro IBM i
- z/OS Příklad plánování kanálu zpráv pro z/OS
- z/OS Příklad plánování kanálu zpráv pro z/OS použití skupin sdílení front

Informace o uživatelských procedurách kanálu naleznete v tématu Programy uživatelských procedur kanálu pro kanály systému zpráv.

Související pojmy

"Odesílání a příjem zpráv" na stránce 210
Následující obrázek ukazuje model distribuované správy front s podrobnými informacemi o vztazích mezi entitami při přenosu zpráv. Zobrazuje také tok pro řízení.

"Funkce řízení kanálu" na stránce 218
Funkce řízení kanálu poskytuje prostředky pro definování, monitorování a řízení kanálů.

"Co se stane, když zprávu nelze doručit?" na stránce 231
Pokud zprávu nelze doručit, může ji agent MCA zpracovat několika způsoby. Může to zkusit znovu, může to vrátit odesílateli, nebo to může dát do fronty nedoručených zpráv.

"Inicializační a konfigurační soubory" na stránce 236
Zpracování inicializačních dat kanálu závisí na vaší platformě IBM MQ .

"Převod dat pro zprávy" na stránce 237
Zprávy produktu IBM MQ mohou vyžadovat převod dat při odesílání mezi frontami v různých správcích front.

"Psaní vlastních agentů kanálů zpráv" na stránce 238
Produkt IBM MQ vám umožňuje psát vlastní programy MCA (message channel agent) nebo instalovat programy od nezávislého dodavatele softwaru.

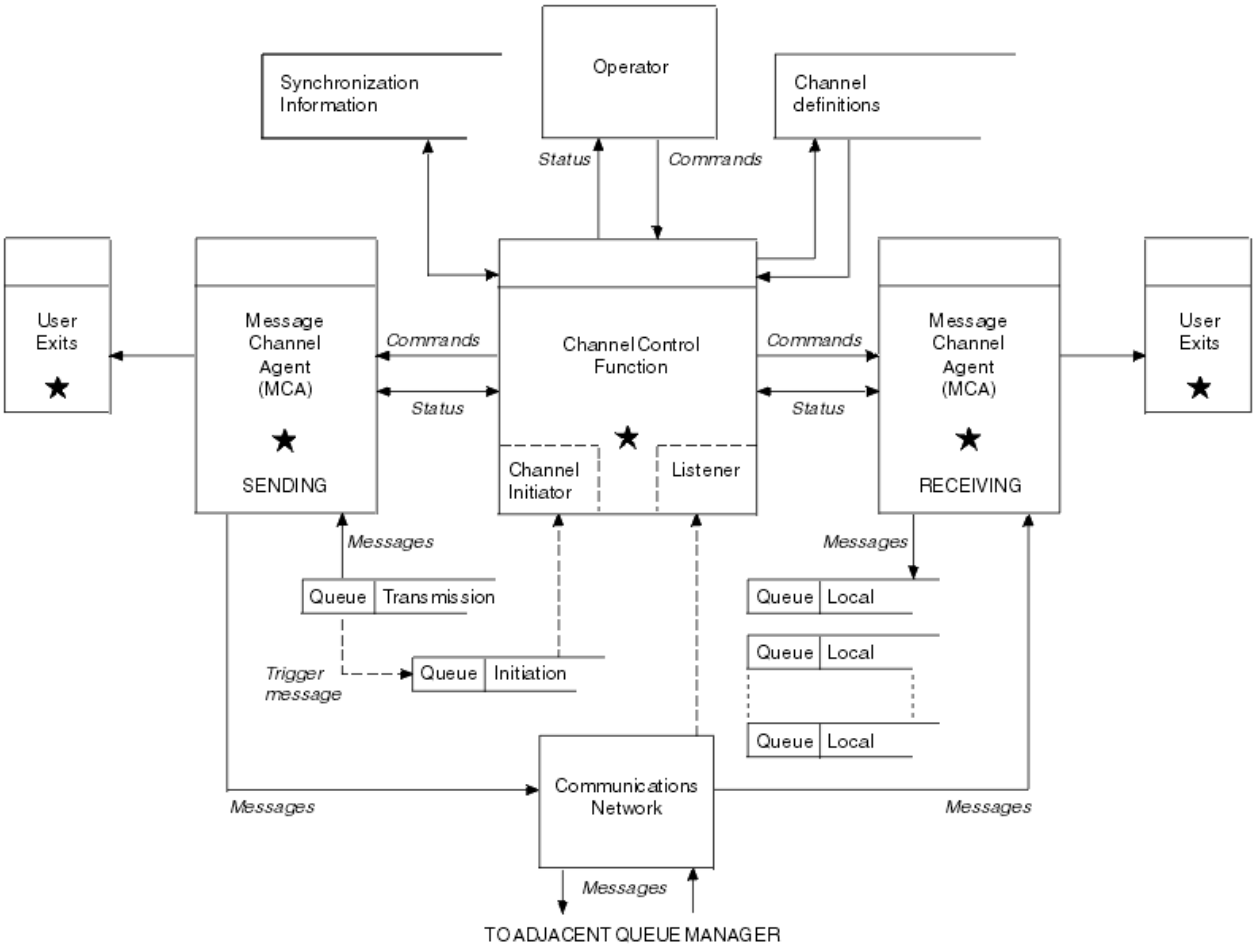
"Další věci, které je třeba zvážit pro správu distribuovaných front" na stránce 238
Další témata, která je třeba zvážit při přípravě produktu IBM MQ pro distribuovanou správu front. Toto téma se týká fronty nedoručených zpráv, používaných front, rozšíření systému a uživatelských programů a spuštěných kanálů a modulů listener jako důvěryhodných aplikací.

Související odkazy

Příklad informací o konfiguraci

Odesílání a příjem zpráv

Následující obrázek ukazuje model distribuované správy front s podrobnými informacemi o vztazích mezi entitami při přenosu zpráv. Zobrazuje také tok pro řízení.



Obrázek 15. Model správy distribuovaných front

Poznámka:

1. K dispozici je jeden MCA na kanál, v závislosti na platformě. Pro konkrétního správce front může existovat jedna nebo více funkcí řízení kanálu.
2. Implementace MCA a funkcí řízení kanálů je vysoce závislá na platformě. Může se jednat o programy, procesy nebo podprocesy a může se jednat o jeden objekt nebo o mnoho z nich, které se skládají 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:

- Je-li spuštěn příkazem, je název kanálu předán v datové oblasti. Agent MCA poté načte definici kanálu přímo, aby získal její atributy.
- Pro odesílatele a v některých případech pro kanály serveru může být agent MCA spuštěn automaticky spouštěčem správce front. Název kanálu je načten z definice procesu spouštěče, kde je to možné, a předán do agenta MCA. Zbývající zpracování je stejné jako dříve popsané. Kanály serveru musí být nastaveny tak, aby spouštěly pouze v případě, že jsou plně kvalifikované, tj. uvádějí název CONNAME, ke kterému se mají připojit.
- Pokud je kanál spuštěn vzdáleně odesílatelem, serverem, žadatelem nebo připojením klienta, je název kanálu předán v počátečních datech z agenta kanálu zpráv partnera. Agent MCA čte definici kanálu přímo, aby získal její atributy.

Určité atributy, které nejsou definovány v definici kanálu, jsou také převoditelné:

Rozdělit zprávy
Pokud jeden konec nepodporuje zprávy rozdělení, pak se zprávy rozdělení neodešlou.

Schopnost převodu
Pokud jeden konec nemůže v případě potřeby provést nezbytný převod kódové stránky nebo převod číselného kódování, druhý konec ji musí zpracovat. Pokud jej nepodporuje ani jeden konec, kanál nelze v případě potřeby spustit.

Podpora seznamu distribuce
Pokud jeden konec nepodporuje distribuční seznamy, partnerský agent MCA nastaví příznak ve své přenosové frontě tak, aby věděl, že zachytává zprávy určené pro více cílů.

Stav kanálu a pořadová čísla

Programy agenta kanálu zpráv uchovávají záznamy aktuálního pořadového čísla a čísla logické pracovní jednotky pro každý kanál a obecného stavu kanálu. Některé platformy vám umožňují zobrazit tyto informace o stavu, které vám pomohou řídit kanály.

Jak odeslat zprávu jinému správci front

Tento oddíl popisuje nejjednodušší způsob odeslání zprávy mezi správci front, včetně nezbytných předpokladů a požadovaných autorizací. K odesílání zpráv vzdálenému správci front lze použít i jiné metody.

Před odesláním zprávy z jednoho správce front do jiného je třeba provést následující kroky:

1. Zkontrolujte, zda je zvolený komunikační protokol k dispozici.
2. Spusťte správce front.
3. Spusťte iniciátory kanálu.
4. Spusťte listenery.

Také musíte mít správnou autorizaci zabezpečení IBM MQ pro vytvoření požadovaných objektů.

Chcete-li odesílat zprávy z jednoho správce front do jiného, postupujte takto:

- Definujte následující objekty ve zdrojovém správci front:
  - Kanál odesílatele
  - Definice vzdálené fronty
  - Inicializační fronta (z/OS povinná v systému z/OS, jinak volitelná)
  - Přenosová fronta
  - Fronta nedoručených zpráv
- Definujte následující objekty v cílovém správci front:
  - Kanál příjemce
  - Cílová fronta
  - Fronta nedoručených zpráv

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

- Na všech platformách můžete použít příkazy skriptu IBM MQ (MQSC) popsané v části Příkazy MQSC příkazy ve formátu programovatelných příkazů (PCF) popsané v části Automatizace úloh administracenebo v Průzkumníku systému IBM MQ .
- z/OS V systému z/OSmůžete také použít ovládací panely popsané v tématu Administrace IBM MQ for z/OS .
- IBM i V systému IBM imůžete také použít rozhraní panelu.

Další informace o vytváření komponent pro odesílání zpráv jinému správci front naleznete v následujících dílčích tématech:

Související pojmy

“IBM MQ techniky distribuovaného řazení do front” na stránce 190
Dílčí témata v této části popisují techniky, které se používají při plánování kanálů. Tato dílčí témata popisují techniky, které vám pomohou naplánovat, jak spojit správce front dohromady a spravovat tok zpráv mezi aplikacemi.

“Úvod do správy distribuovaných front” na stránce 209
Distribuovaná správa front (DQM) se používá k definování a řízení komunikace mezi správci front.

“Spouštění kanálů” na stránce 233
Produkt IBM MQ poskytuje prostředek pro automatické spuštění aplikace při splnění určitých podmínek ve frontě. Toto zařízení se nazývá spouštění.

“Bezpečnost zpráv” na stránce 231
Kromě typických funkcí zotavení produktu IBM MQzajišťuje správa distribuovaných front správné doručení zpráv pomocí procedury synchronizačního bodu koordinované mezi dvěma konci kanálu zpráv. Pokud tento postup zjistí chybu, zavře kanál, abyste mohli problém vyšetřit, a uchová zprávy bezpečně v přenosové frontě, dokud nebude kanál restartován.

Související úlohy

“Vytvoření správců front na platformě Multiplatforms” na stránce 7
Než budete moci používat zprávy a fronty, musíte vytvořit a spustit alespoň jednoho správce front a jeho přidružené objekty. Správce front spravuje přidružené prostředky, zejména fronty, které vlastní. Poskytuje služby řazení do front pro aplikace pro volání rozhraní MQI (Message Queueing Interface) a příkazy pro vytváření, úpravy, zobrazování a odstraňování objektů IBM MQ .

“Monitorování a řízení kanálů na systému AIX, Linux, and Windows” na stránce 240
Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, IBM MQ Explorer, souborů pro definice kanálů a oblasti úložiště pro synchronizační informace.

“Monitorování a řízení kanálů na systému IBM i” na stránce 263
Pomocí panelů a příkazů DQM můžete vytvářet, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení s kompatibilními vzdálenými správci front.

“Konfigurace připojení mezi klientem a serverem” na stránce 14
Chcete-li konfigurovat komunikační spojení mezi produktem IBM MQ MQI clients a servery, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

“Konfigurace klastru správců front” na stránce 284
Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 950
Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

Definování kanálů

Chcete-li odesílat zprávy z jednoho správce front do jiného, musíte definovat dva kanály. Musíte definovat jeden kanál ve zdrojovém správci front a jeden kanál v cílovém správci front.

Ve zdrojovém správci front

Definujte kanál s typem kanálu SENDER. Musíte uvést následující:

- Název přenosové fronty, která se má použít (atribut XMITQ).
- Název připojení partnerského systému (atribut CONNAME).
- Název používaného komunikačního protokolu (atribut TRPTYPE). V systému IBM MQ for z/OSmusí být protokol TCP nebo LU6.2. Na jiných platformách toto nemusíte zadávat. Můžete ji ponechat pro vyzvednutí hodnoty z 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 stejným názvem jako kanál odesilatele.

Zadejte název používaného komunikačního protokolu (atribut TRPTYPE). V systému IBM MQ for z/OSmusí být protokol TCP nebo LU6.2. Na jiných platformách toto nemusíte zadávat. Můžete ji ponechat pro vyzvednutí hodnoty z výchozí definice kanálu.

Definice přijímacího kanálu mohou být generické. To znamená, že pokud máte několik správců front, kteří komunikují se stejným příjemcem, mohou všechny odesílací kanály zadat stejný název pro příjemce a jedna definice zásobníku se vztahuje na všechny.

Po definování kanálu jej můžete otestovat pomocí příkazu PING CHANNEL. Tento příkaz odešle speciální zprávu z odesílacího kanálu do přijímacího kanálu a zkontroluje, zda je vrácena.

Poznámka: Hodnota parametru TRPTYPE je ignorována odpovídajícím agentem kanálu zpráv. Například TRPTYPE protokolu TCP v definici odesílacího kanálu se úspěšně spustí s TRPTYPE LU62 v definici přijímacího kanálu jako partner.

Definování front

Chcete-li odesílat zprávy z jednoho správce front do jiného, musíte definovat až šest front. Ve zdrojovém správci front je třeba definovat až čtyři fronty a v cílovém správci front až dvě fronty.

Ve zdrojovém správci front

- Definice vzdálené fronty

  V této definici uveďte 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 nemusíte zadávat. Pokud tak neučiníte, použije se přenosová fronta se stejným názvem jako cílový správce front. Pokud neexistuje, použije se výchozí přenosová fronta. Doporučuje se, abyste dali přenosové frontě stejný název jako cílovému správci front, aby byla fronta standardně nalezena.

- Definice inicializační fronty

  z/OS Toto je povinné. Musíte použít inicializační frontu s názvem SYSTEM.CHANNEL.INITQ.

  Multi Toto je volitelné. Zvažte pojmenování inicializační fronty SYSTEM.CHANNEL.INITQ.

- Definice přenosové fronty

  Lokální fronta s atributem USAGE nastaveným na XMITQ. IBM i Pokud používáte nativní rozhraní IBM MQ for IBM i , atribut USAGE je *TMQ.

- Definice fronty nedoručených zpráv

  Definujte frontu nedoručených zpráv, do které lze zapisovat nedoručené zprávy.

V cílovém správci front

- Definice lokální fronty

  Cílová fronta. Název této fronty musí být stejný jako název zadaný 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 215
Před spuštěním kanálu (jiného než žadatelský kanál) musí být přenosová fronta definována podle popisu v této části. Přenosová fronta musí být pojmenována v definici kanálu.

“Vytvoření přenosové fronty v systému IBM i” na stránce 215
Přenosovou frontu můžete vytvořit na platformě IBM i pomocí panelu Vytvořit frontu MQM.

Vytvoření přenosové fronty
Před spuštěním kanálu (jiného než žadatelský kanál) musí být přenosová fronta definována podle popisu v této části. Přenosová fronta musí být pojmenována v definici kanálu.

Definujte lokální frontu s atributem USAGE nastaveným na XMITQ pro každý odesílající kanál zpráv. Chcete-li ve svých definicích vzdálené fronty použít specifickou přenosovou frontu, vytvořte vzdálenou frontu, jak je zobrazeno.

Chcete-li vytvořit přenosovou frontu, použijte příkaz IBM MQ (MQSC), jak je uvedeno v následujících příkladech:

Příklad vytvoření přenosové fronty

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

Příklad vytvoření vzdálené fronty

```
DEFINE QREMOTE(PAYROLL) DESCR('Remote queue for QM2') +
XMITQ(QM2) RNAME(PAYROLL) RQMNAME(QM2)
```

Zvažte pojmenování přenosové fronty názvem správce front ve vzdáleném systému, jak je uvedeno v příkladech.

Vytvoření přenosové fronty v systému IBM i
Přenosovou frontu můžete vytvořit na platformě IBM i pomocí panelu Vytvořit frontu MQM.

Pro každý odesílající kanál zpráv musíte definovat lokální frontu s atributem pole Použití nastaveným na hodnotu *TMQ.

Chcete-li použít definice vzdálené fronty, použijte stejný příkaz k vytvoření fronty typu *RMT a použití *NORMAL.

Chcete-li vytvořit přenosovou frontu, použijte příkaz CRTMQMQ z příkazového řádku k zobrazení prvního panelu pro vytvoření fronty; viz Obrázek 16 na stránce 216.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Queue name . . . . . .

Queue type . . . . . .  ____     *ALS, *LCL, *MDL, *RMT

Message Queue Manager name . . .  *DFT_____________________________
_____









Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
+
```

Obrázek 16. Vytvořit frontu (1)

Zadejte název fronty a zadejte typ fronty, kterou chcete vytvořit: Lokální, Vzdálený nebo Alias. Pro přenosovou frontu uveďte na tomto panelu Lokální (*LCL) a stiskněte klávesu Enter.

Zobrazí se druhá stránka panelu Vytvořit frontu MQM. Viz Obrázek 17 na stránce 216.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Queue name . . . . . > HURS.2.HURS.PRIORIT

Queue type . . . . . > *LCL     *ALS, *LCL, *MDL, *RMT
Message Queue Manager name . . .  *DFT
Replace . . . . . .  *NO      *NO, *YES
Text 'description' . . . . . .  '                  '
Put enabled . . . . . .  *YES     *SYSDFTQ, *NO, *YES
Default message priority . . . .  0       0-9, *SYSDFTQ
Default message persistence . .  *NO      *SYSDFTQ, *NO, *YES
Process name . . . . . .  '                  '
Triggering enabled . . . . . .  *NO      *SYSDFTQ, *NO, *YES
Get enabled . . . . . .  *YES     *SYSDFTQ, *NO, *YES
Sharing enabled . . . . . .  *YES     *SYSDFTQ, *NO, *YES




More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 17. Vytvořit frontu (2)

Změňte libovolnou ze zobrazených výchozích hodnot. Stisknutím klávesy Page down přejděte na další obrazovku; viz Obrázek 18 na stránce 217.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Default share option . . . . . *YES     *SYSDFTQ, *NO, *YES
Message delivery sequence . . .  *PTY     *SYSDFTQ, *PTY, *FIFO
Harden backout count . . . . . *NO      *SYSDFTQ, *NO, *YES
Trigger type . . . . . *FIRST    *SYSDFTQ, *FIRST, *ALL...
Trigger depth . . . . . 1       1-999999999, *SYSDFTQ
Trigger message priority . . . . 0       0-9, *SYSDFTQ
Trigger data . . . . . '                 '
Retention interval . . . . . 999999999   0-999999999, *SYSDFTQ
Maximum queue depth . . . . . 5000     1-24000, *SYSDFTQ
Maximum message length . . . . . 4194304    0-4194304, *SYSDFTQ
Backout threshold . . . . . 0       0-999999999, *SYSDFTQ
Backout requeue queue . . . . . '                '
Initiation queue . . . . . '                 '



More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 18. Vytvořit frontu (3)

Zadejte ⁎TMQpro přenosovou frontu do pole Použití tohoto panelu a změňte všechny výchozí hodnoty zobrazené v ostatních polích.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Usage . . . . . *TMQ     *SYSDFTQ, *NORMAL, *TMQ
Queue depth high threshold . . .  80      0-100, *SYSDFTQ
Queue depth low threshold . . .  20      0-100, *SYSDFTQ
Queue full events enabled . . .  *YES     *SYSDFTQ, *NO, *YES
Queue high events enabled . . .  *YES     *SYSDFTQ, *NO, *YES
Queue low events enabled . . . .  *YES     *SYSDFTQ, *NO, *YES
Service interval . . . . . 999999999   0-999999999, *SYSDFTQ
Service interval events . . . .  *NONE     *SYSDFTQ, *HIGH, *OK, *NONE
Distribution list support . . .  *NO      *SYSDFTQ, *NO, *YES
Cluster Name . . . . . *SYSDFTQ
Cluster Name List . . . . . *SYSDFTQ
Default Binding . . . . . *SYSDFTQ   *SYSDFTQ, *OPEN, *NOTFIXED




Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 19. Vytvořit frontu (4)

Až budete spokojeni s tím, že pole obsahují správná data, stiskněte klávesu Enter a vytvořte frontu.

Spuštění kanálu

Vložíte-li zprávy do vzdálené fronty definované ve zdrojovém správci front, budou uloženy do přenosové fronty až do spuštění kanálu. Po spuštění kanálu jsou zprávy doručeny do cílové fronty ve vzdáleném správci front.

Spusťte kanál v odesílajícím správci front pomocí příkazu START CHANNEL. Při spuštění odesílacího kanálu je přijímací kanál spuštěn automaticky (modulem listener) a zprávy jsou odesílány do cílové fronty. Pro přenos zpráv musí být spuštěny oba konce kanálu zpráv.

Protože se oba konce kanálu nacházejí v různých správcích front, mohly být definovány s různými atributy. Chcete-li vyřešit případné rozdíly, dochází k počátečnímu vyjednávání dat mezi oběma konci

při spuštění kanálu. Obecně platí, že oba konce kanálu pracují s atributy, které potřebují méně prostředků. To umožňuje, aby větší systémy pojaly menší prostředky menších systémů na druhém konci kanálu zpráv.

Odesílající agent MCA rozdělí velké zprávy před jejich odesláním přes kanál. Jsou znovu sestaveny ve vzdáleném správci front. To není uživateli zřejmé.

Agent MCA může přenášet zprávy pomocí více podprocesů. Tento proces s názvem *pipelining* umožňuje agentovi MCA efektivněji přenášet zprávy s menším počtem stavů čekání. Pipelining zlepšuje výkon kanálu.

Funkce řízení kanálu

Funkce řízení kanálu poskytuje prostředky pro definování, monitorování a řízení kanálů.

Příkazy jsou vydávány prostřednictvím panelů, programů nebo z příkazového řádku do funkce řízení kanálu. Rozhraní panelu také zobrazuje stav kanálu a data definice kanálu. Můžete použít programovatelné formáty příkazů nebo příkazy IBM MQ (MQSC) a řídicí příkazy, které jsou podrobně popsány v tématu “Monitorování a řízení kanálů na systému AIX, Linux, and Windows” na stránce 240.

Příkazy spadají do následujících skupin:

- Administrace kanálů
- Řízení kanálu
- Monitorování stavu kanálu

Příkazy administrace kanálů se zabývají definicemi kanálů. Umožňují vám:

- Vytvořit definici kanálu
- Kopírovat definici kanálu
- Změnit definici kanálu
- Odstranit definici kanálu

Příkazy pro řízení kanálů spravují činnost kanálů. Umožňují vám:

- Spuštění kanálu
- Zastavení kanálu
- Znovu synchronizovat s partnerem (v některých implementacích)
- Resetovat pořadová čísla zpráv
- Vyřešit nejistou dávku zpráv
- Ping; odeslání testovací komunikace přes kanál

Monitorování kanálů zobrazuje stav kanálů, například:

- Aktuální nastavení kanálu
- Zda je kanál aktivní nebo neaktivní
- Zda byl kanál ukončen v synchronizovaném stavu

Související pojmy

Kde najít informace, které vám pomohou s určením problému

Příprava kanálů

Před pokusem o spuštění kanálu zpráv nebo kanálu MQI je třeba kanál připravit. Musíte se ujistit, že všechny atributy lokálních a vzdálených definic kanálů jsou správné a kompatibilní.

Atributy kanálu popisují definice a atributy kanálu.

Ačkoli jste nastavili explicitní definice kanálů, vyjednávání kanálů provedená při spuštění kanálu mohou přepsat jednu nebo druhou z definovaných hodnot. Toto chování je normální a není uživateli zřejmé a bylo uspořádáno tak, aby jinak nekompatibilní definice mohly spolupracovat.

Automatická definice přijímacích kanálů a kanálů připojení serveru

Pokud v systému IBM MQ na všech platformách kromě platformy z/OSneexistuje žádná odpovídající definice kanálu, pak pro kanál připojení serveru nebo příjemce, který má povolenou automatickou definici, se definice vytvoří automaticky. Definice je vytvořena pomocí:

1. Odpovídající definice kanálu modelu, SYSTEM.AUTO.RECEIVERnebo SYSTEM.AUTO.SVRCONN. Definice kanálu modelu pro automatickou definici jsou stejné jako výchozí nastavení systému SYSTEM.DEF.RECEIVERa SYSTEM.DEF.SVRCONN, s výjimkou pole popisu, které je "Auto-defined by" následované 49 mezerami. Administrátor systému se může rozhodnout změnit libovolnou část dodaných definic kanálu modelu.
2. Informace z partnerského systému. Hodnoty od partnera jsou použity pro název kanálu a hodnotu zalamování pořadového čísla.
3. Program uživatelské procedury kanálu, který lze použít ke změně hodnot vytvořených automatickou definicí. Viz Uživatelský program automatické definice kanálu.

Poté se zkontroluje popis, aby se zjistilo, zda byl změněn uživatelskou procedurou automatické definice, nebo protože byla změněna definice modelu. Pokud je prvních 44 znaků stále "Auto-defined by" následováno 29 mezerami, přidá se název správce front. Pokud je posledních 20 znaků stále prázdné, přidá se místní čas a datum.

Po vytvoření a uložení definice bude spuštění kanálu pokračovat, jako by definice vždy existovala. Velikost dávky, velikost přenosu a velikost zprávy jsou vyjednány s partnerem.

Definování jiných objektů

Před spuštěním kanálu zpráv musí být oba konce definovány (nebo povoleny pro automatickou definici) ve správcích front. Přenosová fronta, kterou má obsluhovat, musí být definována pro správce front na odesílajícím konci. Komunikační spojení musí být definováno a k dispozici. Pro implementaci scénářů popsaných v tématu “Konfigurace distribuovaných front” na stránce 189může být nezbytné připravit další objekty IBM MQ , například definice vzdálených front, definice aliasů správců front a definice aliasů front pro odpovědi.

Informace o definování kanálů MQI viz “Definování kanálů MQI” na stránce 28.

Více kanálů zpráv na jednu přenosovou frontu

Je možné definovat více než jeden kanál na jednu přenosovou frontu, ale pouze jeden z těchto kanálů může být v daném okamžiku aktivní. Tuto volbu zvažte, chcete-li zajistit alternativní trasy mezi správci front pro vyvážení provozu a nápravnou akci selhání propojení. Přenosová fronta nemůže být použita jiným kanálem, pokud předchozí kanál, který ji použil, ukončil ponechání dávky nejistých zpráv na odesílajícím konci. Další informace viz “Zpracování nejistých kanálů” na stránce 229.

Spuštění kanálu

Kanál může být způsoben tím, že začne vysílat zprávy jedním ze čtyř způsobů. Může to 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 (ty kanály, které uvádějí CONNAME). Musíte připravit potřebné objekty pro spuštění kanálů.
- Spuštěno z aplikačního programu (nikoli z přijímacího kanálu, přijímacího kanálu klastru nebo kanálu připojení serveru).
- Spuštěno vzdáleně ze sítě kanálem odesílatele, odesílatele klastru, žadatele, serveru nebo připojení klienta. Tímto způsobem jsou spouštěny kanály příjemce, příjemce klastru a případně server

a žadatelský kanál, stejně jako kanály připojení serveru. Samotné kanály již musí být spuštěny (to znamená, že jsou povoleny).

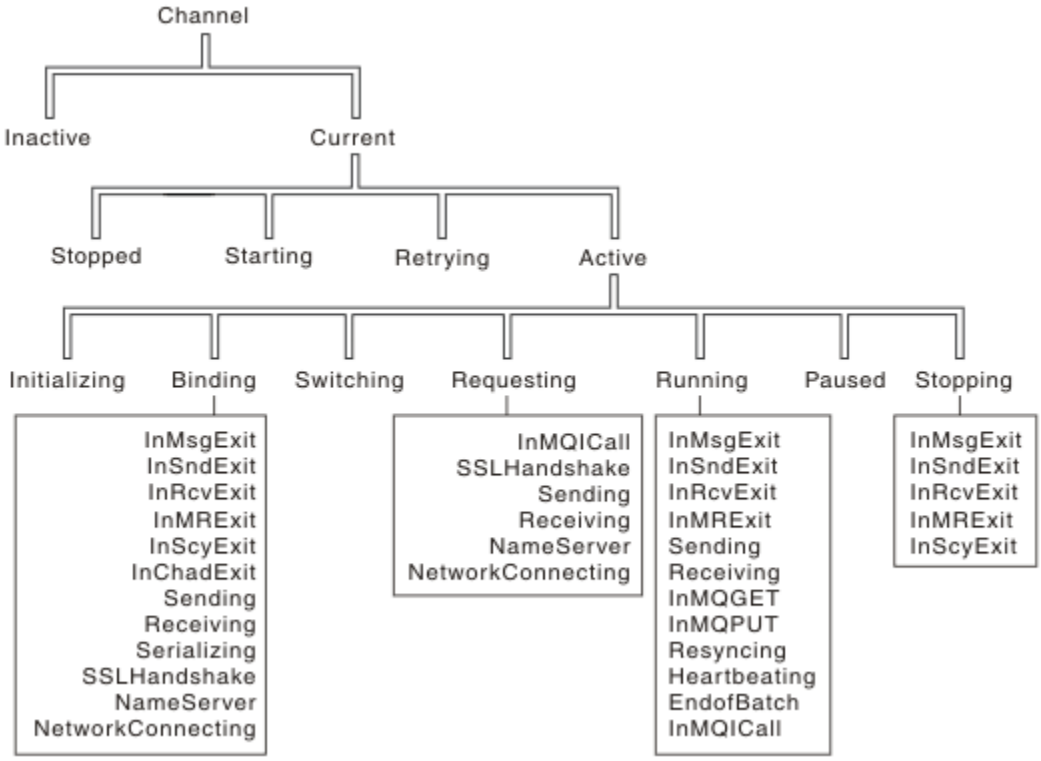
Poznámka: Protože je kanál 'spuštěn', nemusí nutně vysílat zprávy. Místo toho může být 'povoleno' spustit přenos, když dojde k jedné ze čtyř dříve popsaných událostí. Povolení a zakázání kanálu je dosaženo pomocí příkazů operátora START a STOP.

Stavy kanálů

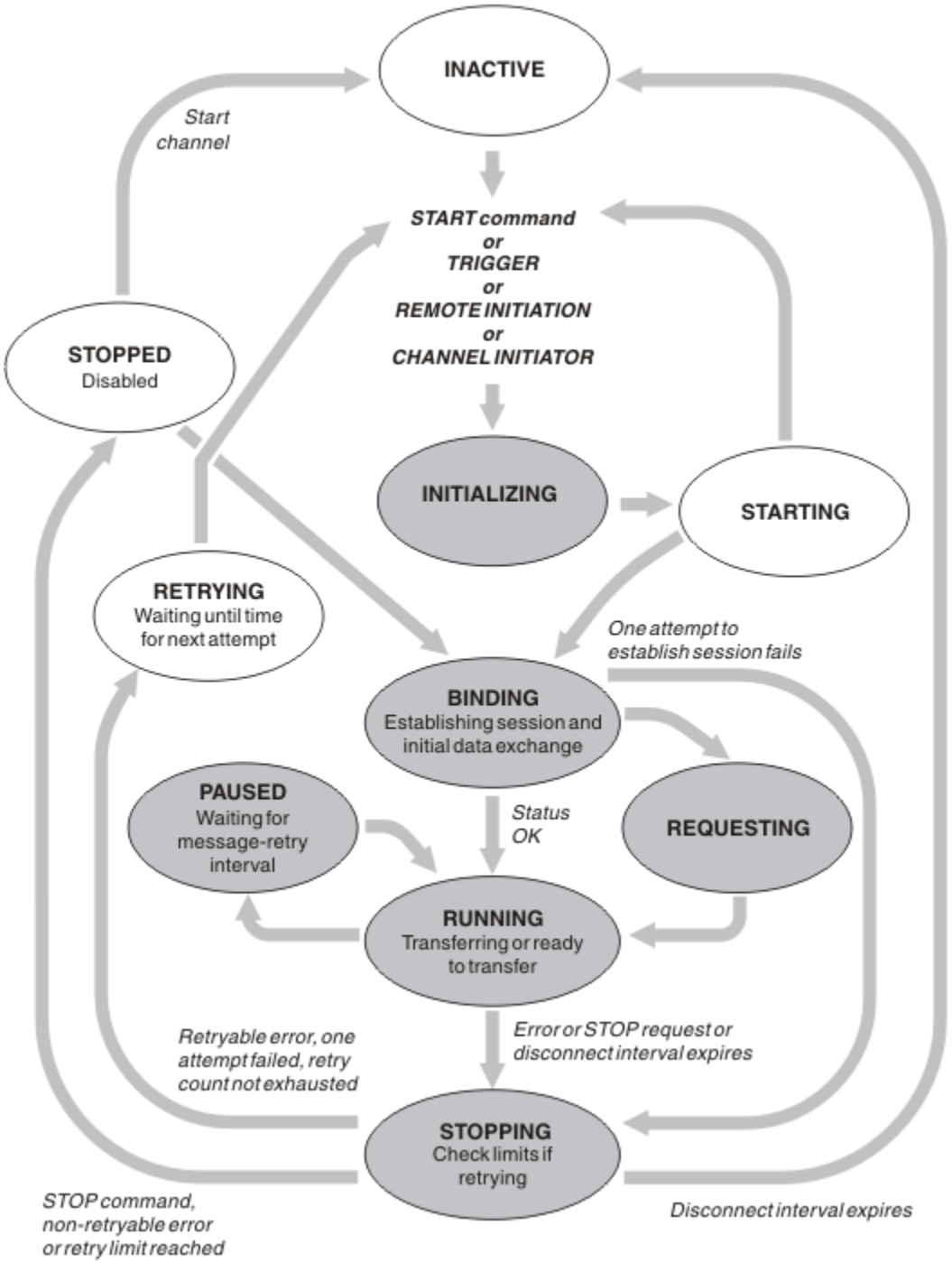
Kanál může být v jednom z mnoha stavů kdykoli. Některé státy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

Obrázek 20 na stránce 220 zobrazuje hierarchii všech možných stavů kanálu a podstavů, které se vztahují na jednotlivé stavy kanálu.

Obrázek 21 na stránce 221 zobrazuje odkazy mezi stavy kanálu. Tyto odkazy se vztahují na všechny typy kanálů kanálu zpráv a kanálů připojení serveru.



Obrázek 20. Stavy a podstavy kanálů



Obrázek 21. Toky mezi stavy kanálu

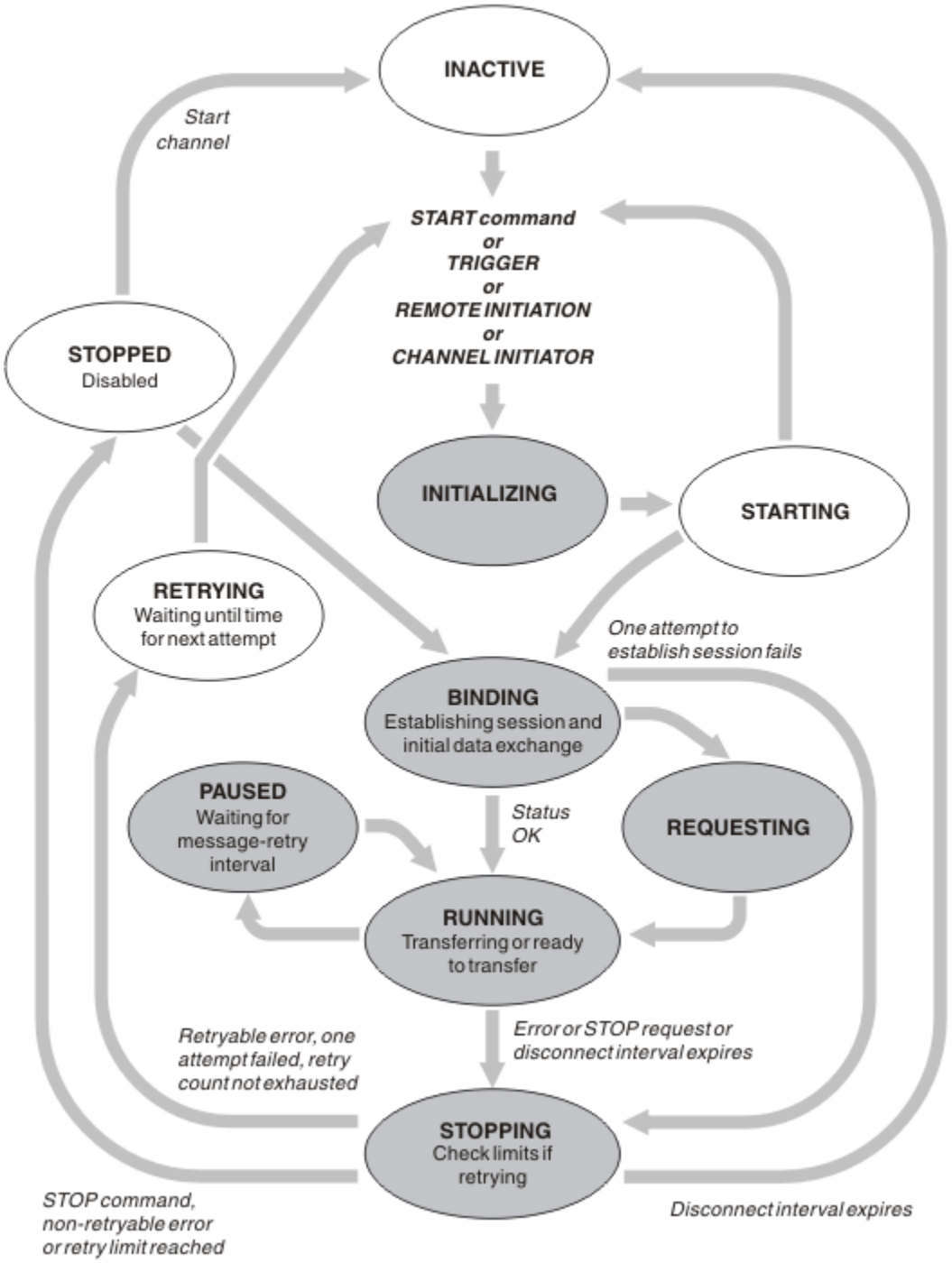
Aktuální a aktivní

Kanál je *aktuální* , pokud je v jiném než neaktivním stavu. Aktuální kanál je *aktivní* , pokud není ve stavu RETRYING, STOPPED nebo STARTING. Když je kanál aktivní, spotřebovává prostředek a proces nebo podproces je spuštěn. V souboru Obrázek 21 na stránce 221je zvýrazněno sedm možných stavů aktivního kanálu (INITIALIZING, BINDING, SPÍNACÍ, POŽADUJÍCÍ, SPUŠTĚNÝ, PAUSED nebo STOPPING).

Aktivní kanál může také zobrazit dílčí stav, který poskytuje podrobnější informace o tom, co přesně kanál dělá. Dílčí stavy pro každý stav jsou zobrazeny v souboru Obrázek 20 na stránce 220.

Aktuální a aktivní
Kanál je "aktuální" , pokud je v jiném než neaktivním stavu. Aktuální kanál je "aktivní" , pokud není ve stavu RETRYING, STOPPED nebo STARTING.

Pokud je kanál "aktivní", může také zobrazit dílčí stav, který poskytuje podrobnější informace o tom, co přesně kanál dělá.



Obrázek 22. Toky mezi stavy kanálu

Poznámka:

1. Nachází-li se kanál v jednom ze šesti stavů zvýrazněných v části Obrázek 22 na stránce 222 (INITIALIZING, BINDING, RUNNING, PAUSED nebo STOPPING), spotřebovává prostředek a je spuštěn proces nebo podproces; kanál je *aktivní*.

2. Je-li kanál ve stavu ZASTAVENO, může být relace aktivní, protože další stav není dosud znám.

Určení maximálního počtu aktuálních kanálů

Můžete určit maximální počet kanálů, které mohou být současně aktuální. Toto číslo je počet kanálů, které mají položky v tabulce stavu kanálu, včetně kanálů, které se opakují, a kanálů, které jsou zastavené. Zadejte tuto hodnotu pro vaši platformu:

- z/OS Použijte příkaz ALTER QMGR MAXCHL .
- IBM i Upravte inicializační soubor správce front.
- Linux AIX Upravte konfigurační soubor správce front.
- Použijte IBM MQ Explorer.

Další informace o hodnotách nastavených pomocí inicializačního nebo konfiguračního souboru naleznete v tématu Sekce konfiguračního souboru pro distribuované fronty. Další informace o určení maximálního počtu kanálů naleznete v následujících tématech:

- ALW Administrace IBM MQ.
- IBM i Administrace IBM MQ for IBM i.
- z/OS Administrace IBM MQ for z/OS.

Poznámka:

1. V tomto počtu jsou zahrnuty kanály připojení serveru.
2. Kanál musí být aktuální, aby se mohl stát aktivním. Pokud je kanál spuštěn, ale nemůže být aktuální, spuštění se nezdaří.

Určení maximálního počtu aktivních kanálů

Můžete také zadat maximální počet aktivních kanálů, abyste zabránili přetížení systému mnoha spouštěnými kanály. Pokud použijete tuto metodu, nastavte atribut intervalu odpojení na nízkou hodnotu, abyste povolili spuštění čekajících kanálů ihned po ukončení ostatních kanálů.

Pokaždé, když se kanál, který se pokouší znovu navázat spojení se svým partnerem, musí se stát aktivním kanálem. Pokud se pokus nezdaří, zůstane aktuálním kanálem, který není aktivní, dokud není čas na další pokus. Počet opakování pokusů kanálu a četnost opakování je určena atributy počtu opakování a intervalu opakování kanálu. Pro oba tyto atributy existují krátké a dlouhé hodnoty. Další informace viz Atributy kanálu .

Má-li se kanál stát aktivním kanálem (protože byl zadán příkaz START nebo byl spuštěn nebo je-li čas na další pokus o opakování), ale nemůže tak učinit, protože počet aktivních kanálů je již na maximální hodnotě, čeká kanál na uvolnění jednoho z aktivních slotů jinou instancí kanálu, která přestane být aktivní. Pokud se však kanál spouští, protože je iniciován vzdáleně, a v té době pro něj nejsou k dispozici žádné aktivní sloty, vzdálená inicializace je odmítnuta.

Kdykoli se kanál jiný než žadatelský kanál pokouší o aktivaci, přejde do stavu STARTING (spouštění). Tento stav nastane i v případě, že je aktivní slot okamžitě k dispozici, i když je ve stavu STARTOVÁNÍ pouze na krátkou dobu. Pokud však kanál musí čekat na aktivní slot, je v době čekání ve stavu STARTING (spouštění).

Kanály žadatele nepřecházejí do stavu STARTING (spouštění). Pokud nelze kanál žadatele spustit, protože počet aktivních kanálů je již omezen, bude ukončen nestandardním způsobem.

Kdykoli kanál jiný než žadatelský kanál nemůže získat aktivní slot, a tak na něj čeká, zapíše se zpráva do protokolu z/OS nebo do konzoly z/OS a vygeneruje se událost. Když je slot později uvolněn a kanál jej může získat, vygeneruje se další zpráva a událost. Žádná z těchto událostí a zpráv není generována, pokud je kanál schopen okamžitě získat slot.

Pokud je zadán příkaz STOP CHANNEL v době, kdy kanál čeká na aktivaci, přejde kanál do stavu ZASTAVENO. Byla vyvolána událost Channel-Stopped.

Kanály připojení serveru jsou zahrnuty do maximálního počtu aktivních kanálů.

Další informace o určení maximálního počtu aktivních kanálů naleznete v následujících tématech:

- ALW Administrace IBM MQ.
- IBM i Administrace IBM MQ for IBM i.
- z/OS Administrace IBM MQ for z/OS.

Chyby kanálu
Chyby na kanálech způsobí, že kanál zastaví další přenosy. Je-li kanál odesilatelem nebo serverem, přejde do stavu RETRY, protože je možné, že se problém sám vyčistí. Pokud nemůže přejít do stavu RETRY, přejde kanál do stavu STOPPED.

Pro odesílací kanály je přidružená přenosová fronta nastavena na GET (DISABLED) a spouštění je vypnuto. (Příkaz STOP s STATUS (STOPPED) přejde na stranu, která jej vydala do stavu STOPPED; pouze vypršení intervalu odpojení nebo příkaz STOP s STATUS (INACTIVE) způsobí, že bude ukončen normálně a stane se neaktivním.) Kanály, které jsou ve stavu STOPPED, potřebují zásah operátora, aby mohly být restartovány (viz “Restartování zastavených kanálů” na stránce 229).

Poznámka: V systémech IBM i IBM i, AIX, Linux, and Windows musí být spuštěn inicializátor kanálu, aby bylo možné pokus zopakovat. Není-li inicializátor kanálu k dispozici, stane se kanál neaktivní a musí být ručně restartován. Používáte-li ke spuštění kanálu skript, ujistěte se, že je inicializátor kanálu spuštěn, než se pokusíte spustit skript.

Počet dlouhých opakování (LONGRTY) popisuje, jak opakování funguje. Pokud se chyba vymaže, kanál se automaticky restartuje a přenosová fronta se znovu povolí. Je-li dosaženo limitu opakování bez vymazání chyb, kanál přejde do stavu ZASTAVENO. Zastavený kanál musí být ručně restartován operátorem. Je-li chyba stále přítomna, neopakuje se znovu. Když se úspěšně spustí, přenosová fronta se znovu povolí.

z/OS Pokud se iniciátor kanálu zastaví v době, kdy je kanál ve stavu RETRYING nebo STOPPED, stav kanálu se při restartování inicializátoru kanálu zapamatuje. Avšak stav kanálu pro typ kanálu SVRCONN je resetován, pokud se iniciátor kanálu zastaví, když je kanál ve stavu ZASTAVENO.

Multi Pokud se správce front zastaví v době, kdy je kanál ve stavu RETRYING nebo STOPPED, stav kanálu se při restartování správce front zapamatuje. Od roku IBM MQ 8.0 to platí i pro kanály SVRCONN. Dříve byl stav kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

Pokud kanál nemůže vložit zprávu do cílové fronty, protože je tato fronta plná nebo zablokovaná, může zopakovat operaci několikrát (specifikováno v atributu počet opakování zprávy) v časovém intervalu (specifikovaném v atributu interval opakování zprávy). Případně můžete napsat vlastní uživatelskou proceduru opakování zprávy, která určí, které okolnosti způsobí opakování, a počet provedených pokusů. Kanál přejde do stavu PAUSED během čekání na dokončení intervalu opakování zprávy.

Informace o atributech kanálu naleznete v tématu Atributy kanálu a informace o uživatelské proceduře pro opakování zpráv naleznete v tématu Programy uživatelské procedury pro kanály systému zpráv .

Omezení kanálu připojení serveru

Můžete nastavit omezení kanálu připojení serveru, abyste zabránili aplikacím klienta vyčerpat prostředky kanálu správce front pomocí parametru **MAXINST** , a zabránit jedné aplikaci klienta v vyčerpání kapacity kanálu připojení serveru pomocí parametru **MAXINSTC** .

MAXINST a **MAXINSTC** nastavíte pomocí příkazu **DEFINE CHANNEL** .

Maximální celkový počet kanálů může být kdykoli aktivní v jednotlivých správcích front. Celkový počet instancí kanálu připojení serveru je zahrnut v maximálním počtu aktivních kanálů.

Pokud neuvedete maximální počet souběžných instancí kanálu připojení serveru, který lze spustit, pak je možné pro jednu klientskou aplikaci připojující se k jednomu kanálu připojení serveru vyčerpat maximální počet aktivních kanálů, které jsou k dispozici. Po dosažení maximálního počtu aktivních kanálů zabrání spuštění všech ostatních kanálů ve správci front. Chcete-li se této situaci vyhnout, musíte omezit počet souběžných instancí jednotlivého kanálu připojení serveru, který lze spustit, bez ohledu na to, který klient je spustil.

Je-li hodnota limitu snížena pod aktuálně spuštěný počet instancí kanálu připojení serveru, a to i na nulu, nebudou spuštěné kanály ovlivněny. Nové instance nelze spustit, dokud nebude ukončen dostatečný počet existujících instancí, aby byl počet aktuálně spuštěných instancí menší než hodnota limitu.

Také mnoho různých kanálů připojení klienta se může připojit k jednotlivým kanálům připojení serveru. Omezení počtu souběžných instancí jednotlivého kanálu připojení serveru, který lze spustit, bez ohledu na to, který klient je spustil, brání jakémukoli klientovi vyčerpat maximální aktivní kapacitu kanálu správce front. Pokud také neomezíte počet souběžných instancí jednotlivého kanálu připojení serveru, který lze spustit z jednotlivého klienta, pak je možné, aby jedna chybná klientská aplikace otevřela tolik připojení, že vyčerpá kapacitu kanálu přidělenou individuálnímu kanálu připojení serveru, a tím zabrání ostatním klientům, kteří potřebují kanál používat, aby se k němu připojovali. Chcete-li se této situaci vyhnout, musíte omezit počet souběžných instancí jednotlivého kanálu připojení serveru, který lze spustit z jednotlivého klienta.

Je-li hodnota omezení počtu jednotlivých klientů nižší než počet instancí kanálu připojení serveru, které jsou aktuálně spuštěny z jednotlivých klientů, a to i na nulu, nebudou spuštěné kanály ovlivněny. Nové instance kanálu připojení serveru však nelze spustit z jednotlivého klienta, který překračuje nový limit, dokud nepřestane běžet dostatečný počet existujících instancí z tohoto klienta, takže počet aktuálně spuštěných instancí je menší než hodnota tohoto parametru.

Související odkazy

Atributy kanálů a typy kanálů

Definovat kanál

Kontrola, zda je druhý konec kanálu stále k dispozici

Pomocí intervalu prezenčního signálu, intervalu udržení aktivity a časového limitu příjmu můžete zkontrolovat, zda je druhý konec kanálu k dispozici.

Prezenční signály

Pomocí atributu kanálu intervalu prezenčního signálu můžete určit, že toky mají být předávány z odesílajícího agenta MCA v případě, že v přenosové frontě nejsou žádné zprávy, jak je popsáno v tématu Interval prezenčního signálu (HBINT).

Ponechat aktivní

z/OS Pokud v systému z/OSpoužíváte protokol TCP/IP jako přenosový protokol, můžete také zadat hodnotu pro atribut **Keepalive** interval channel (**KAINT**). Doporučuje se, abyste dali intervalu **Keepalive** vyšší hodnotu, než je interval prezenčního signálu, a nižší hodnotu, než je hodnota odpojení. Tento atribut můžete použít k určení hodnoty časového limitu pro každý kanál, jak je popsáno v tématu Interval udržení aktivity (KAINT).

Multi Pokud v systémech IBM i, AIX, Linux, and Windows používáte jako přenosový protokol protokol TCP, můžete nastavit `keepalive=yes`. Pokud uvedete tuto volbu, TCP pravidelně kontroluje, zda je druhý konec připojení stále k dispozici. Není, kanál je ukončen. Tato volba je popsána v části Interval udržení aktivity (KAINT).

Pokud máte nespolehlivé kanály, které hlásí chyby TCP, použití volby **Keepalive** znamená, že vaše kanály budou s větší pravděpodobností obnoveny.

Můžete určit časové intervaly pro řízení chování volby **Keepalive** . Změníte-li časový interval, budou ovlivněny pouze kanály TCP/IP spuštěné po změně. Ujistěte se, že hodnota, kterou zvolíte pro časový interval, je menší než hodnota intervalu odpojení pro kanál.

Další informace o použití volby **Keepalive** viz parametr **KAINT** v příkazu **DEFINE CHANNEL** .

Časový limit pro příjem

Používáte-li jako přenosový protokol protokol TCP, bude přijímající konec nečinného připojení kanálu jiného než MQI uzavřen také v případě, že po určitou dobu nebudou přijata žádná data. Toto období, hodnota *vypršení časového limitu pro příjem* , se určuje podle hodnoty **HBINT** (interval prezenčního signálu).

V systémech IBM MQ for IBM i, AIX, Linux, and Windows je hodnota *vypršení časového limitu příjmu* nastavena takto:

1. Pro počáteční počet toků je před jakýmkoli vyjednáváním hodnota *vypršení časového limitu příjmu* dvojnásobkem hodnoty **HBINT** z definice kanálu.
2. Jakmile kanály vyjednají hodnotu **HBINT** , pokud je hodnota **HBINT** nastavena na méně než 60 sekund, hodnota *vypršení časového limitu příjmu* se nastaví na dvojnásobek této hodnoty. Je-li parametr **HBINT** nastaven na 60 sekund nebo více, hodnota *vypršení časového limitu příjmu* je nastavena na 60 sekund větší než hodnota HBINT.

z/OS V systému z/OSje hodnota *vypršení časového limitu příjmu* nastavena takto:

1. Pro počáteční počet toků je před jakýmkoli vyjednáváním hodnota *vypršení časového limitu příjmu* dvojnásobkem hodnoty **HBINT** z definice kanálu.
2. Je-li nastavena hodnota **RCVTIME** , je časový limit nastaven na jednu z následujících hodnot, v závislosti na parametru **RCVTTYPE** , a pokud se použije parametr **RCVTMIN** , podléhá jakémukoli omezení:
   - Vyjednaný HBINT vynásobený konstantou
   - Vyjednaný HBINT plus konstantní počet sekund
   - Konstantní počet sekund

   RCVTMIN se nepoužije, když je nakonfigurován produkt **RCVTTYPE(EQUAL)** . Pokud použijete konstantní hodnotu **RCVTIME** a použijete interval prezenčního signálu, neuvádějte hodnotu **RCVTIME** menší než interval prezenčního signálu. Podrobnosti o atributech **RCVTIME**, **RCVTMIN** a **RCVTTYPE** viz příkaz **ALTER QMGR** .

Poznámka:

1. Je-li jedna z hodnot nula, časový limit nevyprší.
2. Pro připojení, která nepodporují prezenční signály, je hodnota **HBINT** v kroku 2 vyjednána na nulu, a proto neexistuje žádný časový limit, takže musíte použít volbu TCP/IP KEEPALIVE.
3. U připojení klienta, která používají sdílení konverzací, mohou prezenční signály protékat kanálem (z obou stran) po celou dobu, a to nejen v případě, že je operace MQGET neprovedená.
4. U připojení klienta, kde nejsou používány konverzace sdílení, jsou synchronizační signály ze serveru proudeny pouze v případě, že klient zadá volání MQGET s čekáním. Proto se nedoporučuje nastavit interval prezenčního signálu příliš malý pro kanály klienta. Pokud je například prezenční signál nastaven na hodnotu 10 sekund, volání MQCMIT selže (s hodnotou MQRC_CONNECTION_BROKEN), pokud potvrzení trvá déle než 20 sekund, protože během této doby nebyla žádná data přenášena. To se může stát s velkými pracovními jednotkami. K tomu však nedojde, pokud jsou pro interval prezenčního signálu vybrány příslušné hodnoty, protože pouze operace MQGET s čekáním trvá delší časové období.

   Za předpokladu, že hodnota **SHARECNV** není nula, klient použije plně duplexní připojení, což znamená, že klient může (a může) prezenční signál během všech volání MQI
5. Zrušení připojení po uplynutí dvojnásobku intervalu prezenčního signálu je platné, protože je očekáván tok dat nebo synchronizačních signálů alespoň v každém intervalu prezenčního signálu. Nastavení příliš malého intervalu prezenčního signálu však může způsobit problémy, zejména pokud používáte uživatelské procedury kanálu. Je-li například hodnota **HBINT** jedna sekunda a je-li použita uživatelská

procedura odeslání nebo příjmu, čeká přijímající strana před zrušením kanálu pouze 2 sekundy. Pokud agent MCA provádí úlohu, jako je například šifrování zprávy, může být tato hodnota příliš krátká.

Navrhovaná nastavení

z/OS IBM MQ for z/OS

Jako počáteční počáteční bod můžete použít:

```
/cpf ALTER QMGR TCPKEEP(YES) RCVTTYPE(ADD) RCVTIME(60) ADOPTMCA(ALL) ADOPTCHK(ALL)
```

kde `cpf` je předpona příkazu pro subsystém správce front.

Další informace o různých parametrech viz **ALTER QMGR** a IBM MQ dostupnost sítě .

Pokud se adresa IP odesilatele může přeložit na více než jednu adresu, možná budete muset nastavit **ADOPTCHK** na QMNAME namísto ALL.

Multi IBM MQ for Multiplatforms

Do souboru `qm.ini`přidejte následující informace:

```
TCP:
KeepAlive=Yes
CHANNELS:
AdoptNewMCA=ALL
AdoptNewMCACheck=ALL
```

Další informace viz **ALTER QMGR**, Sekce konfiguračního souboru pro distribuované frontya “Sekce kanálů souboru qm.ini” na stránce 115 .

Pokud by adresa IP odesílatele mohla být přeložená na více než jednu adresu, možná budete muset nastavit **AdoptNewMCACheck** na hodnotu QMNAME a nikoli **ALL**.

Adoptování agenta MCA

Funkce Adoptovat agenta MCA umožňuje produktu IBM MQ zrušit kanál příjemce a místo něj spustit nový kanál.

Pokud kanál ztratí kontakt, může být přijímací kanál ponechán ve stavu 'příjem komunikace'. Po opětovném navázání komunikace se kanál odesilatele pokusí znovu navázat spojení. Pokud vzdálený správce front zjistí, že přijímací kanál je již spuštěn, nepovolí spuštění jiné verze téhož přijímacího kanálu. Tento problém vyžaduje zásah uživatele k nápravě problému nebo použití funkce udržení aktivity systému.

Funkce Adoptovat agenta MCA problém řeší automaticky. Umožňuje produktu IBM MQ zrušit přijímací kanál a místo něj spustit nový kanál.

Související úlohy

Správa serveruIBM MQ

Správa serveruIBM MQ for z/OS

Správa serveruIBM MQ for IBM i

Zastavení a uvedení kanálů do klidového stavu

Kanál můžete zastavit a uvést do klidového stavu před vypršením časového intervalu odpojení.

Kanály zpráv jsou navrženy jako přerušitelná připojení mezi správci front s řádným ukončením řízeným pouze atributem kanálu intervalu odpojení. Tento mechanismus funguje dobře, pokud operátor nepotřebuje ukončit kanál před vypršením časového intervalu odpojení. Tato potřeba může nastat v následujících situacích:

- Uvedení systému do klidového stavu
- Ochrana zdrojů

- Jednostranná akce na jednom konci kanálu

V tomto případě můžete kanál zastavit. Můžete to provést pomocí:

- Příkaz STOP CHANNEL MQSC
- příkaz Stop Channel PCF
- průzkumník IBM MQ
- z/OS IBM i jiné mechanismy specifické pro platformu:

  z/OS **Pro z/OS:**
  Panel Zastavit kanál

  IBM i **Pro IBM i:**
  CL příkaz ENDMQMCHL nebo volba END na panelu WRKMQMCHL

Existují tři volby pro zastavení kanálů pomocí těchto příkazů:

QUIESCE
Volba QUIESCE se pokusí ukončit aktuální dávku zpráv před zastavením kanálu.

Vynutit
Volba FORCE se pokusí okamžitě zastavit kanál a může vyžadovat opětovnou synchronizaci kanálu při jeho restartování, protože kanál může být ponechán v nejistém stavu.

z/OS V systému IBM MQ for z/OSpříkaz FORCE přeruší veškeré probíhající realokace zpráv, které mohou zanechat zprávy BIND_NOT_FIXED částečně realokované nebo mimo pořadí.

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

z/OS V systému IBM MQ for z/OSpříkaz TERMINATE přeruší veškerá probíhající realokace zpráv, což může způsobit, že zprávy BIND_NOT_FIXED budou částečně realokovány nebo budou mimo pořadí.

Všechny tyto volby ponechávají kanál ve stavu ZASTAVENO a vyžadují zásah operátora, aby jej restartoval.

Zastavení kanálu na odesílajícím konci je efektivní, ale vyžaduje zásah operátora, aby se restartoval. Na přijímacím konci kanálu je situace mnohem obtížnější, protože agent MCA čeká na data z odesílající strany a neexistuje způsob, jak zahájit *řádné* ukončení kanálu z přijímající strany; příkaz stop čeká na vyřízení, dokud se agent MCA nevrátí z čekání na data.

V důsledku toho existují tři doporučené způsoby použití kanálů v závislosti na požadovaných provozních vlastnostech:

- Pokud chcete, aby vaše kanály byly dlouho spuštěny, všimněte si, že může dojít k řádnému ukončení pouze z odesílajícího konce. Když jsou kanály přerušeny, tj. zastaveny, je nutný zásah operátora (příkaz START CHANNEL), aby bylo možné je restartovat.
- Chcete-li, aby byly kanály aktivní pouze v případě, že existují zprávy pro jejich přenos, nastavte interval odpojení na poměrně nízkou hodnotu. Výchozí nastavení je vysoké, a proto se nedoporučuje pro kanály, pro které je tato úroveň řízení vyžadována. Vzhledem k tomu, že je obtížné přerušit přijímací kanál, nejúspornější možností je, aby se kanál automaticky odpojil a znovu připojil podle požadavků pracovní zátěže. U většiny kanálů lze heuristicky stanovit vhodné nastavení intervalu odpojení.
- Atribut intervalu prezenčního signálu můžete použít k tomu, abyste způsobili, že odesílající agent MCA odešle tok prezenčního signálu přijímajícímu adaptéru MCA během období, ve kterých nemá žádné zprávy k odeslání. Tato akce uvolní přijímající modul MCA ze stavu čekání a umožní mu uvést kanál do klidového stavu bez čekání na vypršení intervalu odpojení. Poskytněte nižší hodnotu intervalu prezenčního signálu, než je hodnota intervalu odpojení.

  Poznámka:

  1. Doporučuje se nastavit interval odpojení na nízkou hodnotu nebo používat prezenční signály pro kanály serveru. Tato nízká hodnota umožňuje případ, kdy je kanál žadatele ukončen nestandardním způsobem (například proto, že byl zrušen) v případě, že pro kanál serveru nejsou k dispozici žádné

zprávy k odeslání. Pokud je interval odpojení nastaven na vysokou hodnotu a prezenční signály nejsou používány, server nezjistí, že žadatel skončil (což provede pouze při dalším pokusu o odeslání zprávy žadateli). Zatímco je server stále spuštěn, zadržuje přenosovou frontu otevřenou pro výlučný vstup, aby získal další zprávy, které dorazí do fronty. Pokud se pokusíte restartovat kanál od žadatele, požadavek na spuštění obdrží chybu, protože server má stále otevřenou přenosovou frontu pro výlučný vstup. Je nutné zastavit kanál serveru a poté znovu spustit kanál od žadatele.

Restartování zastavených kanálů

Když kanál přejde do stavu ZASTAVENO, musíte kanál restartovat ručně.

Informace o této úloze

V případě kanálů odesilatele nebo serveru byla při vstupu kanálu do stavu STOPPED (zastaveno) přidružená přenosová fronta nastavena na hodnotu GET (DISABLED) a spouštění bylo nastaveno na hodnotu GET (DISABLED). Když je přijat požadavek na spuštění, tyto atributy se automaticky vynulují.

z/OS Pokud se iniciátor kanálu zastaví v době, kdy je kanál ve stavu RETRYING nebo STOPPED, stav kanálu se při restartování inicializátoru kanálu zapamatuje. Avšak stav kanálu pro typ kanálu SVRCONN je resetován, pokud se iniciátor kanálu zastaví, když je kanál ve stavu ZASTAVENO.

Multi Pokud se správce front zastaví v době, kdy je kanál ve stavu RETRYING nebo STOPPED, stav kanálu se při restartování správce front zapamatuje. Od roku IBM MQ 8.0 to platí i pro kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

Procedura

- Restartujte kanál jedním z následujících způsobů:
  - Pomocí příkazu START CHANNEL MQSC.
  - Pomocí příkazu Spustit kanál PCF.
  - Pomocí agentaIBM MQ Explorer
  - z/OS V systému z/OSpomocí volby Spustit panel kanálu.
  - IBM i V systému IBM ipomocí příkazu STRMQMCHL CL nebo volby START na panelu WRKMQMCHL.

Zpracování nejistých kanálů

Nejistý kanál je kanál, který je nejistý se vzdáleným kanálem, o kterém byly odesílány a přijímány zprávy.

Informace o této úloze

Všimněte si rozdílu mezi tímto a správcem front, který má pochybnosti o tom, které zprávy by měly být potvrzeny do fronty.

Pomocí parametru kanálu Batch Heartbeat (**BATCHHB**) můžete snížit možnost nejistého umístění kanálu. Je-li zadána hodnota tohoto parametru, kanál odesilatele před provedením dalších akcí zkontroluje, zda je vzdálený kanál stále aktivní. Není-li přijata žádná odpověď, je přijímací kanál považován za neaktivní. Zprávy lze odvolat a přesměrovat a odesílací kanál není uveden do nejistého stavu. Tím se zkrátí doba, po kterou může být kanál nejistý, na dobu mezi odesílacím kanálem, který ověřuje, zda je přijímací kanál stále aktivní, a ověřením, že přijímací kanál přijal odeslané zprávy. Další informace o parametru prezenčního signálu dávky viz Atributy kanálu .

Problémy s neověřeným kanálem jsou obvykle vyřešeny automaticky. I když je komunikace ztracena a kanál je nejistý s dávkou zpráv u odesílatele s neznámým stavem příjmu, je situace vyřešena, když je komunikace znovu zavedena. Pro tento účel se uchovávají záznamy LUWID a pořadová čísla. Kanál je nejistý, dokud nedojde k výměně informací LUWID, a pouze jedna dávka zpráv může být pro kanál nejistá.

V případě potřeby můžete kanál znovu synchronizovat ručně. Termín manuál zahrnuje použití operátorů nebo programů, které obsahují příkazy pro správu systému IBM MQ . Proces ruční resynchronizace funguje následovně. Tento popis používá příkazy MQSC, ale můžete také použít ekvivalenty PCF.

Postup

1. Použijte příkaz **DISPLAY CHSTATUS** k nalezení naposledy potvrzeného ID logické pracovní jednotky (LUWID) pro každou stranu kanálu.

   Proveďte to pomocí následujících příkazů:

   - Pro nejistou stranu kanálu:

     ```
     DISPLAY CHSTATUS(name) SAVED CURLUWID
     ```

     K další identifikaci kanálu můžete použít parametry **CONNAME** a **XMITQ** .

   - Pro přijímací stranu kanálu:

     ```
     DISPLAY CHSTATUS( name ) SAVED LSTLUWID
     ```

     K další identifikaci kanálu můžete použít parametr **CONNAME** .

   Poznámka: Příkazy se liší, protože pouze odesílající strana kanálu může být nejistá. Přijímající strana není nikdy na pochybách.

   IBM i V systému IBM ilze příkaz **DISPLAY CHSTATUS** spustit ze souboru pomocí příkazu **STRMQMMQSC** nebo CL příkazu Práce se stavem kanálu MQM **WRKMQMCHST**.

2. Pokud jsou dva identifikátory LUWID stejné, použijte příkaz **RESOLVE CHANNEL** k potvrzení neověřených zpráv.

   Pokud jsou dva LUWID stejné, přijímající strana potvrdí transakci, kterou odesilatel považuje za nejistou. Odesílající strana může nyní odebrat nejisté zprávy z přenosové fronty a znovu je povolit. To se provádí pomocí následujícího příkazu **RESOLVE CHANNEL** :

   ```
   RESOLVE CHANNEL(name) ACTION(COMMIT)
   ```

3. Pokud se tyto dva identifikátory LUWID liší, použijte příkaz **RESOLVE CHANNEL** k vrácení neověřených zpráv zpět.

   Pokud se oba LUWID liší, přijímající strana nepotvrdí transakci, kterou odesilatel považuje za nejistou. Odesílající strana musí uchovat neověřené zprávy v přenosové frontě a znovu je odeslat. To se provádí pomocí následujícího příkazu **RESOLVE CHANNEL** :

   ```
   RESOLVE CHANNEL( name ) ACTION(BACKOUT)
   ```

   IBM i V systému IBM imůžete použít příkaz Vyřešit kanál MQM **RSVMQMCHL**.

Výsledky

Po dokončení tohoto procesu již není kanál v nejistém stavu. Přenosovou frontu nyní může v případě potřeby používat jiný kanál.

Související odkazy

DISPLAY CHSTATUS (zobrazení stavu kanálu)

RESOLVE CHANNEL (požádat kanál o vyřešení neověřených zpráv)

Bezpečnost zpráv

Kromě typických funkcí zotavení produktu IBM MQzajišťuje správa distribuovaných front správné doručení zpráv pomocí procedury synchronizačního bodu koordinované mezi dvěma konci kanálu zpráv. Pokud tento postup zjistí chybu, zavře kanál, abyste mohli problém vyšetřit, a uchová zprávy bezpečně v přenosové frontě, dokud nebude kanál restartován.

Procedura synchronizačního bodu má další přínos v tom, že se pokusí obnovit situaci *nejistého* při spuštění kanálu. (*Nejistý* je stav jednotky zotavení, pro kterou byl vyžádán synchronizační bod, ale výsledek požadavku není dosud znám.) K tomuto zařízení jsou přidruženy také tyto dvě funkce:

1. Vyřešit s potvrzením nebo odvolání
2. Resetovat pořadové číslo

Použití těchto funkcí se vyskytuje pouze za výjimečných okolností, protože kanál se ve většině případů automaticky obnoví.

Rychlé, přechodné zprávy

Pomocí atributu kanálu NPMSPEED (rychlost dočasných zpráv) lze určit, že mají být všechny přechodné zprávy kanálu doručovány rychleji. Další informace o tomto atributu naleznete v tématu Rychlost dočasných zpráv (NPMSPEED).

Pokud se kanál ukončí během rychlého přenosu přechodných zpráv, mohou být zprávy ztraceny a je na aplikaci, aby v případě potřeby uspořádala jejich obnovu.

Pokud přijímající kanál nemůže vložit zprávu do své cílové fronty, je umístěna do fronty nedoručených zpráv, pokud byla definována. Pokud ne, zpráva se zruší.

Poznámka: Pokud druhý konec kanálu tuto volbu nepodporuje, kanál běží normální rychlostí.

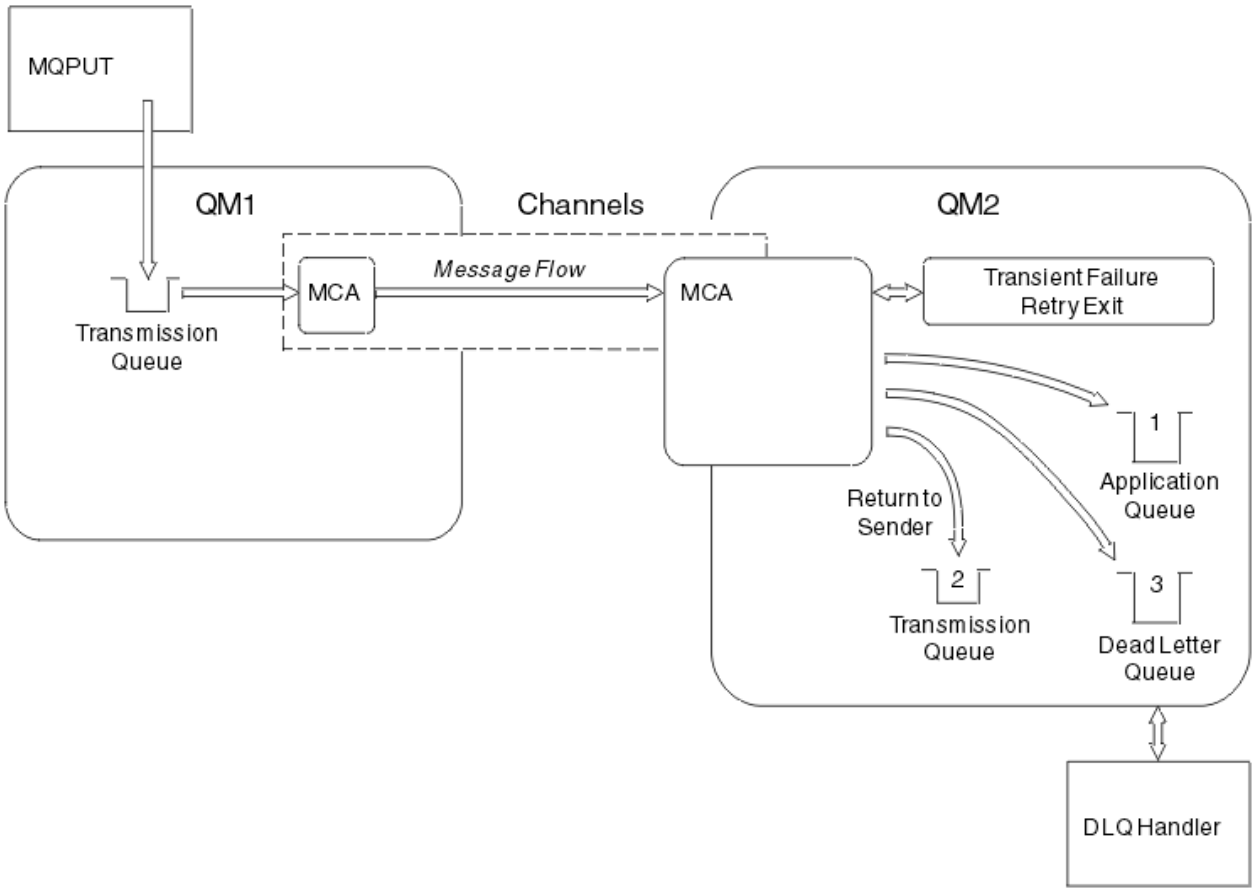
Nedoručené zprávy

Informace o tom, co se stane, když zprávu nelze doručit, viz “Co se stane, když zprávu nelze doručit?” na stránce 231.

Co se stane, když zprávu nelze doručit?

Pokud zprávu nelze doručit, může ji agent MCA zpracovat několika způsoby. Může to zkusit znovu, může to vrátit odesílateli, nebo to může dát do fronty nedoručených zpráv.

Obrázek 23 na stránce 232 zobrazuje zpracování, které se vyskytne, když MCA nemůže vložit zprávu do cílové fronty. (Zobrazené volby se nevztahují na všechny platformy.)



Obrázek 23. Co se stane, když zprávu nelze doručit

Jak je znázorněno na obrázku, agent MCA může provést několik akcí se zprávou, kterou nemůže doručit. Prováděná akce je určena volbami určenými při definování kanálu a volbami sestavy MQPUT pro zprávu.

1. opakování zprávy

   Pokud agent MCA nemůže vložit zprávu do cílové fronty z důvodu, který by mohl být přechodný (například z důvodu zaplnění fronty), může agent MCA počkat a zopakovat operaci později. Můžete určit, zda agent MCA čeká, jak dlouho a kolikrát se o to pokusí.

   - Při definování kanálu můžete určit dobu opakování zpráv a interval pro chyby MQPUT. Pokud zprávu nelze vložit do cílové fronty, protože fronta je plná nebo je blokována pro vložení, agent MCA se pokusí o operaci v zadaném časovém intervalu.
   - Můžete napsat vlastní uživatelskou proceduru opakování zprávy. Uživatelská procedura vám umožňuje určit, za jakých podmínek má agent MCA zkusit operaci MQPUT nebo MQOPEN znovu. Při definování kanálu zadejte název uživatelské procedury.

2. vrátit odesilateli

   Pokud byl pokus o zopakování zprávy neúspěšný nebo byl zjištěn jiný typ chyby, může agent MCA odeslat zprávu zpět původci. Chcete-li povolit návrat odesilatele, musíte v deskriptoru zprávy při vložení zprávy do původní fronty zadat následující volby:

   - Volba sestavy MQRO_EXCEPTION_WITH_FULL_DATA
   - Volba sestavy MQRO_DISCARD_MSG
   - Název fronty pro odpověď a správce front pro odpověď

   Pokud agent 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 odpověď určené

v původní zprávě. (Pokud se fronta pro odpověď nachází ve stejném správci front jako agent MCA, zpráva se vloží přímo do této fronty, nikoli do přenosové fronty.)

3. Fronta nedoručených zpráv

   Pokud zprávu nelze doručit nebo vrátit, je vložena do fronty nedoručených zpráv (DLQ). Ke zpracování zprávy můžete použít obslužnou rutinu DLQ. Toto zpracování je popsáno v tématu Zpracování zpráv ve frontě nedoručených zpráv pro systémy IBM MQ for UNIX, Linux a Windows a v tématu Obslužný program obslužné rutiny fronty nedoručených zpráv (CSQUDLQH) pro systémy z/OS . Není-li fronta nedoručených zpráv k dispozici, odesílající agent MCA ponechá zprávu v přenosové frontě a kanál se zastaví. V rychlém kanálu jsou ztraceny přechodné zprávy, které nelze zapsat do fronty nedoručených zpráv.

   Pokud v systému IBM WebSphere MQ 7.0není definována žádná lokální fronta nedoručených zpráv, není vzdálená fronta k dispozici nebo není definována a neexistuje žádná vzdálená fronta nedoručených zpráv, kanál odesilatele přejde do fronty RETRY a zprávy jsou automaticky odvolány do přenosové fronty.

Související odkazy

Použití fronty nedoručených zpráv (USEDLQ)

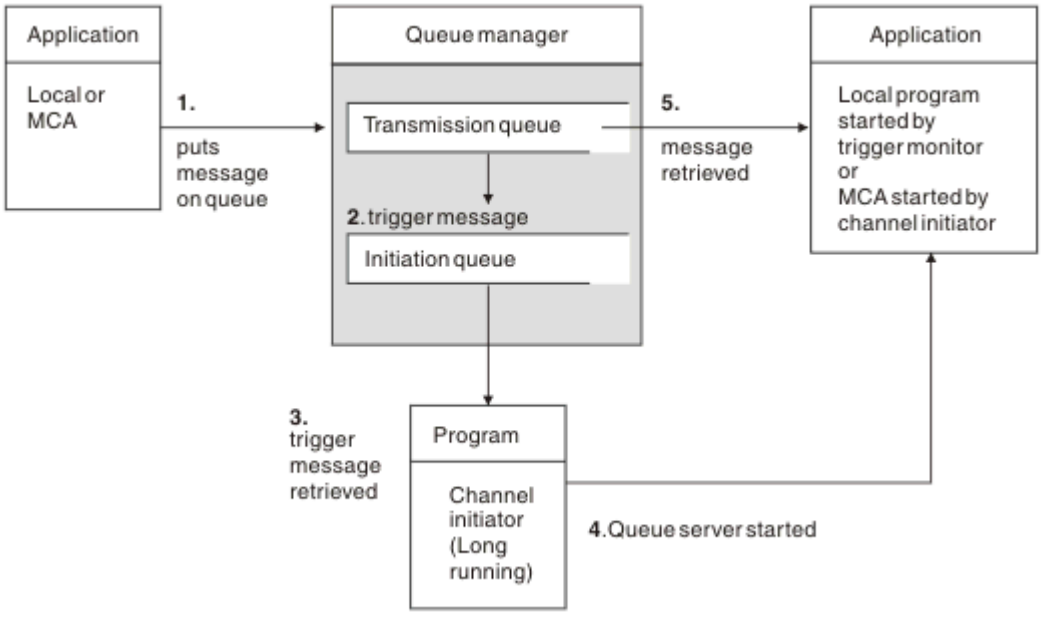
Spouštění kanálů

Produkt IBM MQ poskytuje prostředek pro automatické spuštění aplikace při splnění určitých podmínek ve frontě. Toto zařízení se nazývá spouštění.

Toto vysvětlení je určeno jako přehled spouštěcích konceptů. Úplný popis naleznete v tématu Spuštění aplikací IBM MQ pomocí spouštěčů.

Informace specifické pro platformu viz následující:

- Pro AIX, Linux, and Windowsviz “Spouštění kanálů na systému AIX, Linux, and Windows.” na stránce 234
- IBM i Pro IBM iviz “Spouštění kanálů v adresáři IBM MQ for IBM i” na stránce 235
- z/OS Pro z/OSviz “Přenosové fronty a spouštěcí kanály” na stránce 953



Obrázek 24. Koncepce spouštění

Objekty požadované pro spuštění jsou zobrazeny v souboru Obrázek 24 na stránce 233. Zobrazuje následující posloupnost událostí:

1. Lokální správce front umístí zprávu z aplikace nebo z agenta kanálu zpráv (MCA) do přenosové fronty.
2. Když jsou splněny podmínky spouštěče, lokální správce front umístí zprávu spouštěče do inicializační fronty.
3. Program inicializátoru přerušitelného kanálu monitoruje inicializační frontu a načítá zprávy při jejich doručení.
4. Inicializátor kanálu zpracovává zprávy spouštěče podle informací, které jsou v nich obsaženy. Tyto informace mohou zahrnovat název kanálu. V takovém případě je spuštěn příslušný agent MCA.
5. Lokální aplikace nebo agent MCA, který byl spuštěn, načte zprávy z přenosové fronty.

Chcete-li nastavit tento scénář, musíte:

- Vytvořte přenosovou frontu s názvem inicializační fronty (tj. SYSTEM.CHANNEL.INITQ) v odpovídajícím atributu.
- Ujistěte se, že inicializační fronta (SYSTEM.CHANNEL.INITQ) existuje.
- Ujistěte se, že je program inicializátoru kanálu dostupný a spuštěný. Program inicializátoru kanálu musí být v příkazu pro spuštění uveden s názvem inicializační fronty. z/OS V systému z/OSje název inicializační fronty pevný, takže se nepoužívá v příkazu start.
- Volitelně vytvořte definici procesu pro spuštění, pokud neexistuje, a ujistěte se, že pole *UserData* obsahuje název kanálu, který obsluhuje. Namísto vytvoření definice procesu můžete zadat název kanálu v atributu **TriggerData** přenosové fronty. IBM MQ pro systémy IBM i IBM i, AIX, Linux, and Windows povolte, aby byl název kanálu uveden jako prázdný, v takovém případě se použije první dostupná definice kanálu s touto přenosovou frontou.
- Ujistěte se, že definice přenosové fronty obsahuje název definice procesu, která ji obsluhuje (je-li to možné), název inicializační fronty a spouštěcí charakteristiky, které považujete za nejvhodnější. Atribut řízení spouštěče umožňuje povolit nebo nepovolit spouštění podle potřeby.

Poznámka:

1. Program inicializátoru kanálu se chová jako 'monitor spouštěčů' monitorující inicializační frontu používanou ke spuštění kanálů.
2. Inicializační frontu a proces spouštěče lze použít ke spuštění libovolného počtu kanálů.
3. Lze definovat libovolný počet inicializačních front a procesů spouštěče.
4. Doporučuje se typ spouštěče FIRST, aby se zabránilo zaplavení systému spuštěním kanálu.

Spouštění kanálů na systému AIX, Linux, and Windows.

ALW

V produktu IBM MQmůžete vytvořit definici procesu definující procesy, které mají být spuštěny. Pomocí příkazu MQSC DEFINE PROCESS vytvořte definici procesu, která bude spuštěna při doručení zpráv do přenosové fronty. Atribut USERDATA definice procesu obsahuje název kanálu obsluhovaného přenosovou frontou.

Definujte lokální frontu (QM4) s uvedením, že zprávy spouštěče 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 se má spustit:

```
DEFINE PROCESS(P1) USERDATA(QM3.TO.QM4)
```

Případně můžete pro systémy IBM MQ for UNIX, Linux a Windows 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, ke spuštění aplikace (proces P1), která spouští kanál (QM3.TO.QM4):

```
DEFINE QLOCAL(QM4) TRIGGER INITQ(SYSTEM.CHANNEL.INITQ)
USAGE(XMITQ) TRIGDATA(QM3.TO.QM4)
```

Pokud neuvedete název kanálu, iniciátor kanálu prohledá soubory definice kanálu, dokud nenajde kanál, který je přidružen k pojmenované přenosové frontě.

Spouštění kanálů v adresáři IBM MQ for IBM i

IBM i

Spouštění kanálů v produktu IBM MQ for IBM i je implementováno s procesem inicializátoru kanálu. Proces inicializátoru kanálu pro inicializační frontu SYSTEM.CHANNEL.INITQ se spouští automaticky se správcem front, pokud není zakázán změnou atributu SCHINIT správce front.

Nastavte přenosovou frontu pro kanál s uvedením SYSTEM.CHANNEL.INITQ jako inicializační fronta a povolení spouštěče pro frontu. Inicializátor kanálu spustí první dostupný kanál, který určuje tuto přenosovou frontu.

```
CRTMQMQ QNAME(MYXMITQ1) QTYPE(*LCL) MQMNAME(MYQMGR)
TRGENBL(*YES) INITQNAME(SYSTEM.CHANNEL.INITQ)
USAGE(*TMQ)
```

Deprecated Pomocí příkazu STRMQMCHLI můžete ručně spustit až tři procesy inicializátoru kanálu a zadat různé inicializační fronty. Můžete také zadat více než jeden kanál schopný zpracovat přenosovou frontu a zvolit, který kanál se má spustit. Tato schopnost je stále poskytována, aby byla kompatibilní s dřívějšími verzemi. Jeho použití je zamítnuto.

Poznámka: Přenosovou frontu může v daném okamžiku zpracovat pouze jeden kanál.

```
STRMQMCHLI QNAME(MYINITQ)
```

Nastavte přenosovou frontu pro kanál uvedením TRGENBL (*YES) a pro výběr, který kanál se má spustit, uveďte název kanálu v poli TRIGDATA. Příklad:

```
CRTMQMQ QNAME(MYXMITQ2) QTYPE(*LCL) MQMNAME(MYQMGR)
TRGENBL(*YES) INITQNAME(MYINITQ)
USAGE(*TMQ) TRIGDATA(MYCHANNEL)
```

Související pojmy

“Spuštění a zastavení inicializátoru kanálu” na stránce 236
Spouštění je implementováno pomocí procesu inicializátoru kanálu.

Související úlohy

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

Související odkazy

Programy kanálů na AIX, Linux, and Windows

IBM i Úlohy interkomunikace na systému IBM i

IBM i Stavy kanálů na systému IBM i

Spuštění a zastavení inicializátoru kanálu

Spouštění je implementováno pomocí procesu inicializátoru kanálu.

Tento proces inicializátoru kanálu je spuštěn příkazem MQSC START CHINIT. Pokud nepoužíváte výchozí inicializační frontu, uveďte název inicializační fronty v příkazu. Chcete-li například použít příkaz START CHINIT ke spuštění fronty IQ pro výchozího správce front, zadejte:

```
START CHINIT INITQ(IQ)
```

Při výchozím nastavení je iniciátor kanálu automaticky spuštěn s použitím výchozí inicializační fronty SYSTEM.CHANNEL.INITQ. Chcete-li spustit všechny iniciátory kanálů ručně, postupujte takto:

1. Vytvořte a spusťte správce front.
2. Změnit vlastnost SCHINIT správce front na hodnotu MANUAL
3. Ukončit a restartovat správce front

V systémech IBM MQ for Multiplatforms se iniciátor kanálu spustí 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 AIX and Linux a v registru pro systémy Windows .

Podrobnosti o příkazu spuštění inicializátoru kanálu **runmqchi**a dalších řídicích příkazech viz IBM MQ Řídicí příkazy .

Zastavení inicializátoru kanálu

Výchozí inicializátor kanálu se spustí automaticky při spuštění správce front. Všechny inicializátory kanálu jsou zastaveny automaticky při zastavení správce front.

Inicializační a konfigurační soubory

Zpracování inicializačních dat kanálu závisí na vaší platformě IBM MQ .

IBM MQ for z/OS

z/OS

V produktu IBM MQ for z/OSjsou informace o inicializaci a konfiguraci určeny pomocí příkazu **ALTER QMGR** MQSC. Pokud vložíte příkazy **ALTER QMGR** do vstupní datové sady inicializace CSQINP2 , budou zpracovány při každém spuštění správce front.

Chcete-li spouštět příkazy MQSC, jako např. **START LISTENER** při každém spuštění inicializátoru kanálu, vložte je do vstupní datové sady inicializace CSQINPX a zadejte volitelný příkaz DD CSQINPX v proceduře spuštěné úlohy inicializátoru kanálu.

Další informace o souborech CSQINP2 a CSQINPX naleznete v tématu Úprava vstupních datových sad inicializacea v části ALTER QMGR.

IBM MQ for Multiplatforms

Multi

V produktu IBM MQ for Multiplatformsexistují konfigurační soubory, které uchovávají základní informace o konfiguraci instalace produktu IBM MQ .

Existují dva konfigurační soubory: jeden se týká počítače, druhý se týká jednotlivého správce front.

IBM MQ konfigurační soubor
V tomto souboru jsou uloženy informace týkající se všech správců front v systému IBM MQ . Soubor se nazývá `mqs.ini`. Je popsáno v tématu “IBM MQ konfigurační soubor mqs.ini” na stránce 85.

Konfigurační soubor správce front

Tento soubor obsahuje informace o konfiguraci týkající se jednoho konkrétního správce front. Soubor se nazývá `qm.ini`.

Je vytvořen během vytváření správce front a může obsahovat informace o konfiguraci týkající se libovolného aspektu správce front. Informace uchovávané v souboru zahrnují podrobnosti o tom, jak se konfigurace protokolu liší od výchozí konfigurace v konfiguračním souboru IBM MQ .

Konfigurační soubor správce front je uložen v kořenovém adresáři adresářového stromu obsazeného správcem front. Například pro atributy **DefaultPath** by konfigurační soubory správce front pro správce front s názvem QMNAME byly:

Pro systémy AIX and Linux :

```
/var/mqm/qmgrs/QMNAME/qm.ini
```

Pro systémy Windows :

```
C:\ProgramData\IBM\MQ\qmgrs\QMNAME\qm.ini
```

Pro IBM i:

```
/QIBM/UserData/mqm/qmgrs/QMNAME/qm.ini
```

Zde je výpis z `qm.ini`. Určuje, že modul listener protokolu TCP/IP má naslouchat na portu 2500, maximální počet aktuálních kanálů je 200 a maximální počet aktivních kanálů je 100.

```
TCP:
Port=2500
CHANNELS:
MaxChannels=200
MaxActiveChannels=100
```

Můžete určit rozsah portů TCP/IP, které má odchozí kanál používat. Jednou z metod je použití souboru `qm.ini` k určení začátku a konce rozsahu hodnot portů. Následující příklad ukazuje soubor `qm.ini` uvádějící rozsah kanálů:

```
TCP:
StrPort=2500
EndPort=3000
CHANNELS:
MaxChannels=200
MaxActiveChannels=100
```

Pokud zadáte hodnotu pro **StrPort** nebo **EndPort** , musíte uvést hodnotu pro obojí. Hodnota **EndPort** musí být vždy větší než hodnota **StrPort**.

Kanál se pokusí použít každou hodnotu portu v zadaném rozsahu. Když je připojení úspěšné, hodnota portu je port, který pak kanál používá.

Další informace o souborech `qm.ini` viz “Konfigurační soubory správce front, qm.ini” na stránce 97.

Převod dat pro zprávy

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

Zpráva IBM MQ se skládá ze dvou částí:

- Řídicí informace v deskriptoru zprávy
- Data aplikací

Každá z těchto dvou částí může vyžadovat převod dat při odesílání mezi frontami v různých správcích front. Informace o převodu dat aplikace viz Převod dat aplikace.

Psaní vlastních agentů kanálů zpráv

Produkt IBM MQ vám umožňuje psát vlastní programy MCA (message channel agent) nebo instalovat programy od nezávislého dodavatele softwaru.

Možná budete chtít napsat své vlastní programy MCA, aby IBM MQ spolupracovala s vlastním proprietárním komunikačním protokolem, nebo abyste odesílali zprávy přes protokol, který produkt IBM MQ nepodporuje. (Nemůžete napsat vlastní agenta MCA, který bude spolupracovat s agentem MCA dodaným IBM MQna druhém konci.)

Pokud se rozhodnete použít agenta MCA, který nebyl dodán produktem IBM MQ, musíte zvážit následující body.

Odesílání a příjem zpráv
Musíte napsat odesílající aplikaci, která získá zprávy odkudkoli, kam je vaše aplikace vloží, například z přenosové fronty, a odešle je na protokol, se kterým chcete komunikovat. Musíte také napsat přijímací aplikaci, která převezme zprávy z tohoto protokolu a vloží je do cílových front. Odesílající a přijímající aplikace používají volání rozhraní fronty zpráv (MQI), nikoli žádná speciální rozhraní.

Musíte se ujistit, že jsou zprávy doručeny pouze jednou. Pro pomoc s tímto doručením lze použít koordinaci synchronizačních bodů.

Funkce řízení kanálu
Chcete-li řídit kanály, musíte poskytnout vlastní administrativní funkce. Funkce administrace kanálu IBM MQ nelze použít ani pro konfiguraci (například příkaz DEFINE CHANNEL), ani pro monitorování (například DISPLAY CHSTATUS) kanálů.

Inicializační soubor
Musíte poskytnout svůj vlastní inicializační soubor, pokud jej požadujete.

Převod dat aplikace
Pravděpodobně budete chtít povolit převod dat pro zprávy, které odesíláte na jiný systém. Pokud ano, použijte volbu MQGMO_CONVERT pro volání MQGET při načítání zpráv z libovolného místa aplikace, například z přenosové fronty.

Uživatelské procedury
Zvažte, zda potřebujete uživatelské procedury. Pokud ano, můžete použít stejné definice rozhraní, které používá produkt IBM MQ .

Spouątění
Pokud vaše aplikace vkládá zprávy do přenosové fronty, můžete nastavit atributy přenosové fronty tak, aby byl odesílající agent MCA spuštěn při doručení zpráv do fronty.

Inicializátor kanálu
Možná budete muset poskytnout svůj vlastní inicializátor kanálu.

Další věci, které je třeba zvážit pro správu distribuovaných front

Další témata, která je třeba zvážit při přípravě produktu IBM MQ pro distribuovanou správu front. Toto téma se týká fronty nedoručených zpráv, používaných front, rozšíření systému a uživatelských programů a spuštěných kanálů a modulů listener jako důvěryhodných aplikací.

Nedoručeno-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 může být spouštěn nebo spouštěn v pravidelných intervalech pro zpracování těchto zpráv.

Linux AIX Obslužná rutina DLQ je poskytnuta s IBM MQ na systémech AIX and Linux ; další informace viz Ukázková obslužná rutina DLQ, amqsdlq.

IBM i Další informace o tématu IBM MQ for IBM inaleznete v tématu IBM MQ for IBM i Obslužná rutina fronty nedoručených zpráv.

Používané fronty

MCA pro přijímací kanály mohou ponechat cílové fronty otevřené i v případě, že se zprávy nepřenášejí. To má za následek, že se fronty jeví jako "používané".

Maximální počet kanálů

IBM i V systému IBM MQ for IBM i můžete určit maximální počet kanálů povolených v systému a maximální počet kanálů, které mohou být současně aktivní. Tato čísla určíte v souboru `qm.ini` v adresáři QIBM/UserData/mqm/qmgrs/*název_správce_fronty*. Viz Sekce konfiguračního souboru pro distribuované fronty.

Rozšíření systému a uživatelské programy

V definici kanálu je k dispozici prostředek umožňující spuštění dalších programů v definovaných časech během zpracování zpráv. Tyto programy nejsou dodávány s produktem IBM MQ, ale mohou být poskytnuty každou instalací v souladu s lokálními požadavky.

Aby bylo možné spustit tyto uživatelské programy, musí mít předdefinované názvy a musí být k dispozici na volání programů kanálu. Názvy programů uživatelských procedur jsou zahrnuty v definicích kanálů zpráv.

Existuje definované rozhraní řídicího bloku pro předání řízení těmto programům a pro zacházení s návratem řízení z těchto programů.

Přesná místa, kde jsou tyto programy volány, a podrobnosti o řídicích blocích a názvech jsou k dispozici v části Kanálové uživatelské programy pro kanály systému zpráv.

Spuštění kanálů a modulů listener jako důvěryhodných aplikací

Pokud je výkon ve vašem prostředí důležitý a vaše prostředí je stabilní, můžete spustit kanály a moduly listener jako důvěryhodné pomocí vazby FASTPATH. Existují dva faktory, které ovlivňují, zda jsou kanály a moduly listener spuštěny jako důvěryhodné:

- Proměnná prostředí MQ_CONNECT_TYPE=FASTPATH nebo MQ_CONNECT_TYPE = STANDARD. Rozlišují se velká a malá písmena. Zadáte-li hodnotu, která není platná, bude ignorována.
- MQIBindType v sekci Kanály souboru `qm.ini` nebo registru. Můžete jej nastavit na FASTPATH nebo STANDARD a nerozlišuje velká a malá písmena. Výchozí hodnota je STANDARD.

Můžete použít MQIBindType ve spojení s proměnnou prostředí, abyste dosáhli 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

MQIBindType	Proměnná prostředí	Výsledek
STANDARD	LOKÁLNÍ	STANDARD
Rychlý	LOKÁLNÍ	STANDARD

Stručně řečeno, existují pouze dva způsoby, jak skutečně vytvořit důvěryhodné kanály a moduly listener:

1. Zadáním MQIBindType= FASTPATH v souboru `qm.ini` nebo registru a neurčením proměnné prostředí.
2. Zadáním hodnoty MQIBindType= FASTPATH v souboru `qm.ini` nebo v registru a nastavením proměnné prostředí FASTPATH.

Zvažte spuštění modulů listener jako důvěryhodných, protože moduly listener jsou stabilní procesy. Spuštění kanálů považujte za důvěryhodné, pokud nepoužíváte nestabilní uživatelské procedury kanálu nebo příkaz STOP CHANNEL MODE (TERMINATE).

ALW Monitorování a řízení kanálů na systému AIX, Linux, and Windows

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

Informace o této úloze

K řízení kanálů můžete použít následující typy příkazů:

Příkazy IBM MQ (MQSC)
MQSC můžete použít jako jednotlivé příkazy v relaci MQSC v systémech AIX, Linux, and Windows . Chcete-li zadat složitější nebo více příkazů, může být prostředí MQSC vestavěno do souboru, který poté spustíte z příkazového řádku. Podrobnosti viz Příkazy MQSC. V této části jsou uvedeny některé jednoduché příklady použití prostředí MQSC pro distribuované řazení do front.

Příkazy kanálu jsou podmnožinou příkazů IBM MQ (MQSC). Pomocí MQSC a řídicích příkazů můžete:

- Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálů.
- Spuštění a zastavení kanálů, příkaz ping, resetování pořadových čísel kanálů a vyřešení nejistých zpráv v případě, že odkazy nelze znovu navázat.
- Zobrazit informace o stavu kanálů

Řídicí příkazy
Pro některé z těchto funkcí můžete také zadat *řídicí příkazy* na příkazovém řádku. Podrobnosti naleznete v tématu Administrace IBM MQ for Multiplatforms pomocí řídicích příkazů.

Programovatelné příkazy pro formátování příkazů
Podrobnosti viz Příkazy PCF.

Windows Linux **IBM MQ Explorer**
Na systémech Linux a Windows můžete použít IBM MQ Explorer. To poskytuje grafické administrační rozhraní pro provádění administrativních úloh jako alternativu k použití řídicích příkazů nebo příkazů MQSC. Definice kanálů jsou uchovávány jako objekty správce front.

Každý správce front má komponentu DQM pro řízení propojení s kompatibilními vzdálenými správci front. Oblast úložiště obsahuje pořadová čísla a identifikátory *logické pracovní jednotky (LUW)* . Používají se pro účely synchronizace kanálů.

Seznam funkcí dostupných při nastavování a řízení kanálů zpráv pomocí různých typů příkazů naleznete v části Tabulka 21 na stránce 241.

Procedura

- “Funkce potřebné pro nastavení a ovládání kanálů” na stránce 241
- “Začínáme s objekty” na stránce 243

- “Nastavení komunikace na Windows” na stránce 250
- “Nastavení komunikace na AIX and Linux” na stránce 257

Související úlohy

“Monitorování a řízení kanálů na systému IBM i” na stránce 263
Pomocí panelů a příkazů DQM můžete vytvářet, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení s kompatibilními vzdálenými správci front.

Související odkazy

ALW Programy kanálů na AIX, Linux, and Windows

ALW Příklad plánování kanálu zpráv pro AIX, Linux, and Windows

Příklad informací o konfiguraci
Atributy kanálu

ALW Funkce potřebné pro nastavení a ovládání kanálů

K nastavení a řízení kanálů může být zapotřebí několik funkcí systému IBM MQ . Funkce kanálu jsou vysvětleny v tomto tématu.

Můžete vytvořit definici kanálu s použitím výchozích hodnot dodaných produktem IBM MQ, které určují název kanálu, typ vytvářeného kanálu, použitou komunikační metodu, název přenosové fronty a název připojení.

Název kanálu musí být na obou koncích kanálu stejný a jedinečný v rámci sítě. Avšak musíte omezit znaky použité na ty, které jsou platné pro názvy objektů IBM MQ .

Další funkce související s kanály naleznete v následujících tématech:

- “Začínáme s objekty” na stránce 243
- “Vytvoření přidružených objektů” na stránce 244
- “Vytváření výchozích objektů” na stránce 244
- “Vytvoření kanálu” na stránce 244
- “Zobrazení kanálu” na stránce 245
- “Zobrazení stavu kanálu” na stránce 245
- “Kontrola odkazů pomocí příkazu ping” na stránce 246
- “Spuštění kanálu” na stránce 246
- “Zastavení kanálu” na stránce 247
- “Přejmenování kanálu” na stránce 248
- “Resetování kanálu” na stránce 248
- “Řešení nejistých zpráv v kanálu” na stránce 249

Tabulka 21 na stránce 241 zobrazuje úplný seznam IBM MQ funkcí, které můžete potřebovat.

Tabulka 21. Funkce požadované v systémech AIX, Linux, and Windows

Funkce	**Řídicí příkazy**	**MQSC**	**IBM MQ Ekvivalent průzkumníka?**
Funkce správce front			
Změnit správce front		ALTER QMGR	Ano
Vytvoření správce front	crtmqm		Ano
Odstranit správce front	dltmqm		Ano
Zobrazit správce front		ZOBRAZIT SPRÁVCE FRONT	Ano

Tabulka 21. Funkce požadované v systémech AIX, Linux, and Windows (pokračování)			
Funkce	**Řídicí příkazy**	**MQSC**	**IBM MQ Ekvivalent průzkumníka?**
Ukončit správce front	endmqm		Ano
Odeslat signál Ping pro správce front		PING QMGR	Ne
Spustit správce front	strmqm		Ano
Funkce příkazového serveru			
Zobrazit příkazový server	dspmqcsv		Ne
Ukončit příkazový server	endmqcsv		Ne
Spustit příkazový server	strmqcsv		Ne
Funkce fronty			
Změnit frontu		ALTER QALIAS ALTER QLOCAL ALTER QMODEL ALTER QREMOTE Viz ALTER queues.	Ano
Vymazat frontu		VYMAZAT QLOCAL	Ano
Vytvořit frontu		DEFINE QALIAS DEFINE QLOCAL DEFINE QMODEL DEFINE QREMOTE Viz Fronty DEFINE.	Ano
Odstranit frontu		ODSTRANĚNÍ QALIAS ODSTRANĚNÍ QLOCAL ODSTRANĚNÍ QMODEL ODSTRANĚNÍ QREMOTE Viz Fronty DELETE.	Ano
Fronta zobrazení		FRONTA ZOBRAZENÍ	Ano
funkce procesu			
Změnit proces		ALTER PROCESS	Ano
Vytvořit proces		DEFINOVAT PROCES	Ano
Odstranit proces		Odstranit proces	Ano
Zobrazit proces		PROCES ZOBRAZENÍ	Ano
Funkce kanálů			
Změnit kanál		ALTER CHANNEL	Ano
Vytvořit kanál		Definovat kanál	Ano

Tabulka 21. Funkce požadované v systémech AIX, Linux, and Windows (pokračování)			
Funkce	**Řídicí příkazy**	**MQSC**	**IBM MQ Ekvivalent průzkumníka?**
Odstranit kanál		Odstranit kanál	Ano
Kanál zobrazení		ZOBRAZIT KANÁL	Ano
Zobrazit stav kanálu		ZOBRAZIT STAV	Ano
Koncový 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
Spustit kanál	runmqchl	Spustit kanál	Ano
Spustit inicializátor kanálu	runmqchi	START CHINIT	Ne
Spustit modul listener [1]	runmqlsr	Spustit listener	Ne
Ukončit modul listener	endmqlsr, pouze na následujících platformách: • AIX • Systémy Windows		Ne

Poznámka:

1. Modul listener může být spuštěn automaticky při spuštění správce front.

ALW Začínáme s objekty

Kanály musí být definovány a jejich přidružené objekty musí existovat a být k dispozici pro použití, než bude možné kanál spustit. Tato sekce vám ukáže, jak.

Pomocí příkazů IBM MQ (MQSC) nebo IBM MQ Explorer můžete:

1. Definovat kanály zpráv a přidružené objekty
2. Monitorování a řízení kanálů zpráv

Přidružené objekty, které budete muset definovat, jsou:

- Přenosové fronty
- Definice vzdálené fronty
- Definice aliasů správce front
- Definice aliasu fronty pro odpověď
- Lokální fronty pro odpovědi
- Procesy pro spouštění (MCA)
- Definice kanálů zpráv

Před spuštěním kanálu musí být definováno a k dispozici konkrétní komunikační spojení pro každý kanál. Popis toho, jak jsou definována propojení LU 6.2, TCP/IP, NetBIOS, SPX a DECnet, naleznete v konkrétní komunikační příručce pro vaši instalaci. Viz také Příklad informací o konfiguraci.

Další informace o vytváření a práci s objekty naleznete v následujících dílčích tématech:

ALW *Vytvoření přidružených objektů*

MQSC se používá k vytvoření přidružených objektů.

Pomocí MQSC vytvořte objekty front a aliasů: přenosové fronty, definice vzdálených front, definice aliasů správců front, definice aliasů front pro odpovědi a lokální fronty pro odpovědi.

Také vytvořte definice procesů pro spouštění (MCA) podobným způsobem.

Příklad, jak vytvořit všechny požadované objekty, viz Příklad plánování kanálu zpráv pro produkt AIX, Linux, and Windows.

ALW *Vytváření výchozích objektů*

Výchozí objekty jsou vytvářeny automaticky při vytvoření správce front. Tyto objekty jsou fronty, kanály, definice procesu a administrativní fronty. Po vytvoření výchozích objektů je můžete kdykoli nahradit spuštěním příkazu strmqm s volbou -c.

Použijete-li k vytvoření správce front příkaz crtmqm, příkaz také iniciuje program pro vytvoření sady výchozích objektů.

1. Postupně se vytvoří každý výchozí objekt. Program udržuje počet úspěšně definovaných objektů, počet existujících a nahrazených objektů a počet neúspěšných pokusů.
2. Program vám zobrazí výsledky a pokud se vyskytnou nějaké chyby, přesměruje vás na příslušný protokol chyb, abyste získali podrobnosti.

Po dokončení programu můžete ke spuštění správce front použít příkaz strmqm.

Další informace o příkazech crtmqm a strmqm naleznete v tématu Administrace IBM MQ for Multiplatforms pomocí řídicích příkazů .

Změna výchozích objektů

Zadáte-li volbu -c, bude správce front dočasně spuštěn při vytváření objektů a poté bude znovu ukončen. Zadání příkazu strmqm s volbou -c obnoví existující systémové objekty s výchozími hodnotami (například atribut MCAUSER definice kanálu je nastaven na mezery). Chcete-li spustit správce front, musíte znovu použít příkaz strmqm bez volby -c.

Chcete-li změnit výchozí objekty, můžete vytvořit vlastní verzi starého souboru amqscoma.tst a upravit ji.

ALW *Vytvoření kanálu*

Vytvořte dvě definice kanálů, jednu na každém konci připojení. První definici kanálu vytvoříte v prvním správci front. Poté vytvoříte druhou definici kanálu na druhém správci front na druhém konci odkazu.

Oba konce musí být definovány se stejným názvem kanálu. Oba konce musí mít kompatibilní typy kanálů, například: Odesílatel a přijímač.

Chcete-li vytvořit definici kanálu pro jeden konec odkazu, použijte příkaz MQSC DEFINE CHANNEL. Uveďte název kanálu, typ kanálu pro tento konec připojení, název připojení, popis (v případě potřeby), název přenosové fronty (v případě potřeby) a přenosový protokol. Zahrňte také všechny ostatní atributy, které se mají lišit od systémových výchozích hodnot pro požadovaný typ kanálu, s použitím dříve shromážděných informací.

Je vám poskytnuta pomoc při rozhodování o hodnotách atributů kanálu v poli Atributy kanálu.

Poznámka: Doporučuje se pojmenovat všechny kanály ve vaší síti jedinečně. Dobrým způsobem, jak to provést, je zahrnout názvy zdrojových a cílových správců front do názvu kanálu.

Příklad vytvoření kanálu

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) +
```

```
DESCR('Sender channel to QM2') +
CONNAME(QM2) TRPTYPE(TCP) XMITQ(QM2) CONVERT(YES)
```

Ve všech příkladech MQSC je příkaz zobrazen tak, jak je uveden v souboru příkazů a jak je napsán v souboru AIX, Linux, and Windows. Tyto dvě metody vypadají identicky s tím rozdílem, že chcete-li zadat 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 příkazů na 72 znaků. Použijte znak zřetězení +, jak je zobrazeno, abyste pokračovali přes více než jeden řádek:

- Windows V systému Windows pomocí kombinace kláves Ctrl-z ukončete položku na příkazovém řádku.
- Linux AIX V systému AIX and Linuxpoužijte kombinaci kláves Ctrl-d.
- Případně v systému AIX, Linux, and Windowspoužijte příkaz **end** .

ALW *Zobrazení kanálu*

Pomocí příkazu MQSC DISPLAY CHANNEL zobrazte atributy kanálu.

Parametr ALL příkazu DISPLAY CHANNEL se standardně předpokládá, pokud nejsou požadovány žádné specifické atributy a zadaný název kanálu není generický.

Atributy jsou popsány v části Atributy kanálu.

Příklady zobrazení kanálu

```
DISPLAY CHANNEL(QM1.TO.QM2) TRPTYPE,CONVERT
DISPLAY CHANNEL(QM1.TO.*) TRPTYPE,CONVERT
DISPLAY CHANNEL(*) TRPTYPE,CONVERT
DISPLAY CHANNEL(QM1.TO.QMR34) ALL
```

ALW *Zobrazení stavu kanálu*

Použijte příkaz MQSC DISPLAY CHSTATUS s uvedením názvu kanálu a toho, zda chcete aktuální stav kanálů nebo stav uložených informací.

DISPLAY CHSTATUS platí pro všechny kanály zpráv. Nevztahuje se na jiné kanály MQI než kanály připojení serveru.

Zobrazené informace zahrnují:

- Název kanálu
- Název komunikačního připojení
- Stav nejistoty kanálu (je-li to vhodné)
- Poslední pořadové číslo
- Název přenosové fronty (je-li to vhodné)
- Pochybný identifikátor (je-li to vhodné)
- Poslední potvrzené pořadové číslo
- Identifikátor logické pracovní jednotky
- ID procesu
- Windows ID podprocesu (pouze Windows)

Zobrazit příklady stavu kanálu

```
DISPLAY CHSTATUS(*) CURRENT
DISPLAY CHSTATUS(QM1.TO.*) SAVED
```

Uložený stav se nepoužije, dokud nebude na kanálu přenesena alespoň jedna dávka zpráv. Stav se také uloží při zastavení kanálu (pomocí příkazu STOP CHL) a při ukončení správce front.

ALW *Kontrola odkazů pomocí příkazu ping*

Pomocí příkazu MQSC **PING CHANNEL** vyměňte pevnou datovou zprávu se vzdáleným koncem.

Příkaz ping dává supervizorovi systému určitou jistotu, že odkaz je k dispozici a funguje.

Příkaz ping nezahrnuje použití přenosových front a cílových front. Používá definice kanálů, související komunikační spojení a nastavení sítě. Lze jej použít pouze v případě, že kanál není aktuálně aktivní.

Je k dispozici pouze z odesílacího kanálu, odesílacího kanálu serveru a odesílacího kanálu klastru. Odpovídající kanál je spuštěn na vzdálené straně odkazu a provádí vyjednávání parametrů spuštění. Chyby jsou upozorněny normálně.

Výsledek výměny zpráv se zobrazí jako `Ping complete` nebo jako chybová zpráva.

Příkaz ping s LU 6.2

Při vyvolání příkazu Ping standardně neproudí do přijímacího konce žádné ID uživatele ani heslo. Pokud je vyžadováno ID uživatele a heslo, lze je vytvořit na zahajovacím konci v definici kanálu. Pokud je heslo zadáno do definice kanálu, je před uložením zašifrováno produktem IBM MQ . Poté se dešifruje před tím, než se projde konverzací.

Související úlohy

Použití příkazu ping k testování komunikace

Ověření připojení odesláním signálu ping do kanálu

Související odkazy

PING CHANNEL (odezva testovacího kanálu)

ALW *Spuštění kanálu*

Pro kanály odesilatele, serveru a žadatele použijte příkaz MQSC START CHANNEL. Aby mohly aplikace vyměňovat zprávy, musíte spustit program modulu listener pro příchozí připojení.

Příkaz START CHANNEL není nutný v případě, že byl kanál nastaven se spuštěním správce front.

Při spuštění odesílající agent MCA přečte definice kanálu a otevře přenosovou frontu. Je vydána spouštěcí posloupnost kanálu, která vzdáleně spustí odpovídající MCA kanálu příjemce nebo serveru. Po spuštění odesilatel a procesy serveru čekají na zprávy přicházející do přenosové fronty a odesílají je tak, jak dorazí.

Při použití spouštěcích nebo spouštěcích kanálů jako podprocesů se ujistěte, že je inicializátor kanálu k dispozici pro monitorování inicializační fronty. Iniciátor kanálu je standardně spuštěn jako součást správce front.

Protokoly TCP a LU 6.2 však poskytují další možnosti:

- Linux AIX Pro protokol TCP v systému AIX and Linuxlze inetd nakonfigurovat tak, aby spustil kanál. inetd je spuštěn jako samostatný proces.
- Linux AIX V případě LU 6.2 v produktu AIX and Linuxnakonfigurujte produkt SNA tak, aby spustil proces odpovídacího modulu LU 6.2 .
- Windows V případě LU 6.2 v produktu Windowsmůžete ke spuštění kanálu použít server SNA TpStart (obslužný program poskytovaný se serverem SNA). TpStart je spuštěn jako samostatný proces.

Použití volby Start vždy způsobí opětovnou synchronizaci kanálu, je-li to nutné.

Pro začátek uspět:

- Musí existovat lokální a vzdálené definice kanálů. Pokud neexistuje odpovídající definice kanálu pro příjemce nebo kanál připojení serveru, automaticky se vytvoří výchozí, pokud je kanál automaticky definován. Viz Uživatelský program automatické definice kanálu.
- Přenosová fronta musí existovat a nesmí ji používat žádné jiné kanály.
- Lokální a vzdálené MCA musí existovat.
- Komunikační spojení musí být k dispozici.
- Správci front musí být spuštěni, lokální a vzdálení.
- Kanál zpráv již nesmí být spuštěn.

Na obrazovku se zobrazí zpráva potvrzující, že požadavek na spuštění kanálu byl přijat. Chcete-li potvrdit, že příkaz pro spuštění proběhl úspěšně, zkontrolujte protokol chyb nebo použijte příkaz DISPLAY CHSTATUS. Protokoly chyb jsou:

Windows **Windows**

MQ_DATA_PATH\qmgrs\qmname\errors\AMQERR01.LOG (pro každého správce front s názvem qmname)

MQ_DATA_PATH\qmgrs\@SYSTEM\errors\AMQERR01.LOG (pro obecné chyby)

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

Poznámka: V systému Windowsse i nadále zobrazí zpráva v protokolu událostí systémové aplikace Windows .

Linux AIX **AIX 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 systému AIX, Linux, and Windowspoužijte příkaz **runmqlsr** ke spuštění procesu modulu listener IBM MQ . Při výchozím nastavení všechny příchozí požadavky na připojení kanálu způsobí, že proces modulu listener spustí adaptéry MCA jako podprocesy procesu amqrmppa.

```
runmqlsr -t tcp -m QM2
```

V případě odchozích připojení musíte spustit kanál jedním z následujících tří způsobů:

1. Pomocí příkazu MQSC START CHANNEL, který určuje název kanálu, spusťte kanál jako proces nebo podproces v závislosti na parametru MCATYPE. (Pokud jsou kanály spouštěny jako podprocesy, jedná se o podprocesy inicializátoru kanálu.)

   ```
   START CHANNEL(QM1.TO.QM2)
   ```

2. Ke spuštění kanálu jako procesu použijte řídicí příkaz runmqchl.

   ```
   runmqchl -c QM1.TO.QM2 -m QM1
   ```

3. Ke spuštění kanálu použijte iniciátor kanálu.

ALW ***Zastavení kanálu***

Pomocí příkazu MQSC STOP CHANNEL požádejte kanál o zastavení aktivity. Kanál nespustí novou dávku zpráv, dokud operátor nespustí kanál znovu.

Informace o restartování zastavených kanálů viz “Restartování zastavených kanálů” na stránce 229.

Tento příkaz lze zadat pro kanál libovolného typu s výjimkou MQCHT_CLNTCONN.

Můžete vybrat požadovaný typ zastavení:

Příklad zastavení v klidovém stavu

```
STOP CHANNEL(QM1.TO.QM2) MODE(QUIESCE)
```

Tento příkaz požaduje, aby byl kanál řádně zavíjen. Aktuální dávka zpráv je dokončena a procedura synchronizačního bodu je provedena s druhým koncem kanálu. Je-li kanál nečinný, tento příkaz neukončí přijímací kanál.

Příklad stop force

```
STOP CHANNEL(QM1.TO.QM2) MODE(FORCE)
```

Tato volba okamžitě zastaví kanál, ale neukončí podproces nebo proces kanálu. Kanál nedokončí zpracování aktuální dávky zpráv, a proto může ponechat kanál v nejistém stavu. Obecně zvažte použití volby zastavení uvedení do klidového stavu.

Příklad zastavení ukončení

```
STOP CHANNEL(QM1.TO.QM2) MODE(TERMINATE)
```

Tato volba okamžitě zastaví kanál a ukončí podproces nebo proces kanálu.

Příklad zastavení (uvedení do klidového stavu) zastaveno

```
STOP CHANNEL(QM1.TO.QM2) STATUS(STOPPED)
```

Tento příkaz neuvádí MODE, takže výchozí hodnota je MODE (QUIESCE). Požaduje, aby byl kanál zastaven, takže jej nelze automaticky restartovat, ale musí být spuštěn ručně.

Příklad příkazu Stop (quiesce) inactive

```
STOP CHANNEL(QM1.TO.QM2) STATUS(INACTIVE)
```

Tento příkaz neuvádí MODE, takže výchozí hodnota je MODE (QUIESCE). Požaduje, aby byl kanál deaktivován, aby se automaticky restartoval v případě potřeby.

ALW *Přejmenování kanálu*

K přejmenování kanálu zpráv použijte MQSC.

Pomocí MQSC proveďte následující kroky:

1. Kanál zastavte pomocí příkazu STOP CHANNEL.
2. Pomocí příkazu DEFINE CHANNEL vytvořte duplicitní definici kanálu s novým názvem.
3. Pomocí příkazu DISPLAY CHANNEL zkontrolujte, zda byl správně vytvořen.
4. K odstranění původní definice kanálu použijte příkaz DELETE CHANNEL.

Pokud se rozhodnete přejmenovat kanál zpráv, nezapomeňte, že kanál má dvě definice kanálů, na každém konci jednu. Ujistěte se, že jste přejmenovali kanál na obou koncích současně.

ALW *Resetování kanálu*

Ke změně pořadového čísla zprávy použijte příkaz MQSC RESET CHANNEL.

Příkaz RESET CHANNEL je k dispozici pro všechny kanály zpráv, nikoli však pro kanály MQI (připojení klienta nebo připojení serveru). První zpráva spustí novou posloupnost při příštím spuštění kanálu.

Je-li příkaz zadán na odesílacím kanálu nebo kanálu serveru, informuje druhou stranu o změně při restartování kanálu.

Související pojmy

"Začínáme s objekty" na stránce 243
Kanály musí být definovány a jejich přidružené objekty musí existovat a být k dispozici pro použití, než bude možné kanál spustit. Tato sekce vám ukáže, jak.

"Funkce řízení kanálu" na stránce 218
Funkce řízení kanálu poskytuje prostředky pro definování, monitorování a řízení kanálů.

Související úlohy

"Konfigurace distribuovaných front" na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

Související odkazy

Resetovat kanál

ALW *Řešení nejistých zpráv v kanálu*

Použijte příkaz MQSC RESOLVE CHANNEL, když jsou zprávy zadrženy v nejistém stavu odesilatelem nebo serverem. Například proto, že jeden konec odkazu byl ukončen a není možné, aby se obnovil.

Příkaz RESOLVE CHANNEL přijímá jeden ze dvou parametrů: BACKOUT nebo COMMIT. Volba Backout obnoví zprávy do přenosové fronty, zatímco volba Commit je vyřadí.

Program kanálu se nepokouší ustanovit relaci s partnerem. Místo toho určuje identifikátor logické pracovní jednotky (LUWID), který představuje neověřené zprávy. Poté vydá, jak bylo požadováno, buď:

- BACKOUT pro obnovu zpráv do přenosové fronty; nebo
- COMMIT pro odstranění zpráv z přenosové fronty.

Aby usnesení uspělo:

- Kanál musí být neaktivní
- Kanál musí být nejistý
- Typ kanálu musí být odesilatel, server nebo odesilatel klastru.
- Musí existovat lokální definice kanálu.
- Lokální správce front musí být spuštěn.

Související pojmy

"Začínáme s objekty" na stránce 243
Kanály musí být definovány a jejich přidružené objekty musí existovat a být k dispozici pro použití, než bude možné kanál spustit. Tato sekce vám ukáže, jak.

"Funkce řízení kanálu" na stránce 218
Funkce řízení kanálu poskytuje prostředky pro definování, monitorování a řízení kanálů.

Související úlohy

"Konfigurace distribuovaných front" na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

Související odkazy

Vyřešit kanál

Windows Nastavení komunikace na Windows

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby bylo připojení úspěšné, musí být definováno a k dispozici. Tento oddíl vysvětluje, jak to provést pomocí forem komunikace, které jsou k dispozici pro systémy IBM MQ for Windows .

Než začnete

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

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Informace o této úloze

Při nastavování komunikace pro systém IBM MQ na systému Windowssi můžete vybrat z následujících typů komunikace:

- TCP/IP
- LU 6.2
- NetBIOS

Procedura

- Informace o nastavení komunikace pro systém Windows naleznete v podtématu pro zvolený typ komunikace:
  - “Definování připojení TCP na systému Windows” na stránce 251
  - “Definování připojení LU 6.2 na systému Windows” na stránce 252
  - “Definování připojení NetBIOS na systému Windows” na stránce 254

  Ne všechny funkce a prostředky produktu IBM MQ for Windows jsou k dispozici v prostředích, která používají jiné komunikační protokoly než TCP/IP. Položka, která není k dispozici, je IBM MQ Explorer.

Související úlohy

“Monitorování a řízení kanálů na systému AIX, Linux, and Windows” na stránce 240
Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, IBM MQ Explorer, souborů pro definice kanálů a oblasti úložiště pro synchronizační informace.

“Konfigurace připojení mezi klientem a serverem” na stránce 14
Chcete-li konfigurovat komunikační spojení mezi produktem IBM MQ MQI clients a servery, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

“Nastavení komunikace na AIX and Linux” na stránce 257
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby bylo připojení úspěšné, musí být definováno a k dispozici. Tento oddíl vysvětluje, jak to provést pomocí forem komunikace, které jsou k dispozici pro systémy IBM MQ for UNIX or Linux .

Související odkazy

“Jaký typ komunikace použít” na stránce 15
Různé platformy podporují různé komunikační protokoly. Vaše volba přenosového protokolu závisí na vaší kombinaci platformy IBM MQ MQI client a platformy serveru.

Windows *Definování připojení TCP na systému Windows*

Definujte připojení TCP konfigurací kanálu na odesílajícím konci tak, aby určoval adresu cíle, a spuštěním programu modulu listener na přijímajícím konci.

Než začnete

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Konec odesílání

Do pole Název připojení definice kanálu zadejte název hostitele nebo adresu TCP cílového počítače.

Výchozí hodnota portu pro připojení je 1414. Číslo portu 1414 je přiřazeno autoritou Internet Assigned Numbers k IBM MQ.

Chcete-li použít jiné číslo portu než výchozí, zadejte je do pole názvu připojení definice 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 přijímacím konci.)

Spuštěný kanál musí být zastaven a restartován, aby se projevily jakékoli změny v definici objektu kanálu.

Výchozí číslo portu můžete změnit jeho uvedením v souboru `.ini` pro IBM MQ for Windows:

```
TCP:
Port=1822
```

Poznámka: Chcete-li vybrat, které číslo portu TCP/IP se má použít, produkt IBM MQ použije první číslo portu, které nalezne v následujícím pořadí:

1. Číslo portu explicitně uvedené v definici kanálu nebo v příkazovém řádku. Toto číslo umožňuje přepsání výchozího čísla portu pro kanál.
2. Atribut portu uvedený v sekci TCP souboru `.ini` . Toto číslo umožňuje přepsání výchozího čísla portu pro správce front.
3. Výchozí hodnota je 1414. Jedná se o číslo přiřazené k produktu IBM MQ autoritou Internet Assigned Numbers pro příchozí i odchozí připojení.

Další informace o hodnotách, které jste nastavili pomocí qm.ini, naleznete v části Sekce konfiguračního souboru pro distribuované fronty.

Příjem na TCP

Chcete-li spustit program přijímacího kanálu, musí být spuštěn program modulu listener, který zjišťuje příchozí síťové požadavky a spouští přidružený kanál. Můžete použít modul listener IBM MQ .

Programy přijímacího kanálu jsou spouštěny v reakci na spouštěcí požadavek odesílajícího kanálu.

Chcete-li spustit program přijímacího kanálu, musí být spuštěn program modulu listener, který zjišťuje příchozí síťové požadavky a spouští přidružený kanál. Můžete použít modul listener IBM MQ .

Chcete-li spustit modul listener dodávaný s produktem IBM 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; parametr QMNAME není pro výchozího správce front povinný a číslo portu není vyžadováno, pokud používáte výchozí hodnotu (1414). Číslo portu nesmí být vyšší než 65535.

Poznámka: Chcete-li vybrat, které číslo portu TCP/IP se má použít, produkt IBM MQ použije první číslo portu, které nalezne v následujícím pořadí:

1. Číslo portu explicitně uvedené v definici kanálu nebo v příkazovém řádku. Toto číslo umožňuje přepsání výchozího čísla portu pro kanál.
2. Atribut portu uvedený v sekci TCP souboru `.ini` . Toto číslo umožňuje přepsání výchozího čísla portu pro správce front.
3. Výchozí hodnota je 1414. Jedná se o číslo přiřazené k produktu IBM MQ autoritou Internet Assigned Numbers pro příchozí i odchozí připojení.

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu “Spuštění kanálů a modulů listener jako důvěryhodných aplikací” na stránce 239. Informace o důvěryhodných aplikacích naleznete v tématu Omezení důvěryhodných aplikací .

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 225.

V systému Windowshodnota registru `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` pro volbu Windows **KeepAliveTime** řídí interval, který uplyne před kontrolou připojení. Výchozí hodnota jsou dvě hodiny.

Použití volby nevyřízených požadavků modulu listener TCP

V protokolu TCP se s připojeními zachází jako s neúplnými, pokud mezi serverem a klientem nedojde k třícestnému navázání komunikace. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nevyřízené požadavky čekající na port TCP, aby mohl modul listener přijmout požadavek.

Další informace viz “Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému IBM MQ for Multiplatforms” na stránce 260 a specifická hodnota pro Windows.

Windows *Definování připojení LU 6.2 na systému Windows*

Architektura SNA musí být konfigurována tak, aby bylo možné mezi těmito dvěma počítači navázat konverzaci LU 6.2 .

Jakmile je SNA nakonfigurován, pokračujte následujícím způsobem.

Informace naleznete v následující tabulce.

Tabulka 22. Nastavení v lokálním systému Windows pro vzdálenou platformu správce front		
Vzdálená platforma	**TPNAME**	**TPPATH**
z/OS nebo MVS/ESA bez CICS	Stejné jako v odpovídajících vedlejších informacích o vzdáleném správci front.	-
z/OS nebo MVS/ESA pomocí CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-
IBM i	Stejná hodnota jako porovnávací hodnota v záznamu směrování v systému IBM i .	-
Systémy AIX and Linux	Stejné jako v odpovídajících vedlejších informacích o vzdáleném správci front.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo v vyvolatelném transakčním programu, který byl definován pomocí TpSetup na systému Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

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

Máte-li ve stejném počítači více než jednoho správce front, ujistěte se, že jsou názvy TPname v definicích kanálu jedinečné.

Nejnovější informace o konfiguraci AnyNet SNA přes TCP/IP naleznete v následující online IBM dokumentaci: AnyNet SNA přes TCP/IP a Operace uzlu SNA.

Související pojmy

“Odeslání ukončení na LU 6.2 na Windows” na stránce 253
Vytvořte objekt na straně rozhraní CPI-C (symbolický cíl) z administrační aplikace produktu LU 6.2 , který používáte. Zadejte tento název do pole Název připojení v definici kanálu. Vytvořte také odkaz LU 6.2 na partnera.

“Příjem na logické jednotce 6.2 on Windows” na stránce 253
Programy přijímacího kanálu jsou spouštěny v reakci na spouštěcí požadavek odesílajícího kanálu.

Windows *Odeslání ukončení na LU 6.2 na Windows*

Vytvořte objekt na straně rozhraní CPI-C (symbolický cíl) z administrační aplikace produktu LU 6.2 , který používáte. Zadejte tento název do pole Název připojení v definici kanálu. Vytvořte také odkaz LU 6.2 na partnera.

Do objektu na straně CPI-C zadejte jméno partnerské LU na přijímajícím počítači, jméno TP a jméno režimu. Příklad:

```
Partner LU Name              OS2ROG2
Partner TP Name              recv
Mode Name                    #INTER
```

Windows *Příjem na logické jednotce 6.2 on Windows*

Programy přijímacího kanálu jsou spouštěny v reakci na spouštěcí požadavek odesílajícího kanálu.

Chcete-li spustit program přijímacího kanálu, je třeba spustit program modulu listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program modulu listener spustíte pomocí příkazu RUNMQLSR a zadáte hodnotu TpName pro naslouchání. Alternativně můžete použít TpStart pod serverem SNA pro Windows.

Použití příkazu RUNMQLSR

Příklad příkazu ke spuštění modulu listener:

```
RUNMQLSR -t LU62 -n RECV -m QMNAME
```

kde RECV je TpName , který je uveden na druhém (odesílajícím) konci jako "TpName pro spuštění na vzdálené straně". Parametr **-m** použitý v poslední části tohoto příkazu je volitelný a není vyžadován pro výchozího správce front.

Je možné, aby byl na jednom počítači spuštěn více než jeden správce front. Každému správci front je třeba přiřadit jiný název TpName a poté pro každého z nich spustit program modulu listener. Příklad:

```
RUNMQLSR -t LU62 -m QM1 -n TpName1
RUNMQLSR -t LU62 -m QM2 -n TpName2
```

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu Spuštění kanálů a modulů listener jako důvěryhodných aplikací. Informace o důvěryhodných aplikacích naleznete v tématu Omezení důvěryhodných aplikací .

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

```
ENDMQLSR -m QMNAME
```

Použití Microsoft serveru SNA na Windows

Pomocí příkazu TpSetup (ze sady SDK serveru SNA) můžete definovat vyvolatelné TP, které pak řídí amqcrs6a.exe, nebo můžete ručně nastavit různé hodnoty registru. Parametry, které by měly být předány souboru amqcrs6a.exe , jsou:

```
-m QM -n TpName
```

kde *QM* je název správce front a *TpName* je název TP. Další informace viz příručka *Microsoft SNA Server APPC Programmers Guide* nebo *Microsoft SNA Server CPI-C Programmers Guide* .

Pokud nezadáte název správce front, bude předpokládán výchozí správce front.

Windows *Definování připojení NetBIOS na systému Windows*

Připojení NetBIOS se vztahuje pouze na klienta a server, na kterém běží produkt Windows. Produkt IBM MQ používá při vytváření připojení NetBIOS k jinému produktu IBM MQ tři typy prostředků NetBIOS : relace, příkazy a názvy. Každý z těchto prostředků má limit, který je nastaven buď standardně, nebo podle volby během instalace systému NetBIOS.

Každý spuštěný kanál bez ohledu na typ používá jednu relaci NetBIOS a jeden příkaz NetBIOS . Implementace IBM NetBIOS umožňuje více procesům používat stejný lokální název NetBIOS . Proto musí být pro použití produktem IBM MQk dispozici pouze jeden název NetBIOS . Implementace jiných dodavatelů, například emulace NetBIOS společnosti Novell, vyžadují pro každý proces jiný lokální název. Ověřte vaše požadavky z dokumentace pro produkt NetBIOS , který používáte.

Ve všech případech se ujistěte, že jsou již k dispozici dostatečné prostředky každého typu, nebo zvyšte maximální hodnoty uvedené v konfiguraci. Jakékoli změny hodnot vyžadují restart systému.

Během spouštění systému ovladač zařízení NetBIOS zobrazuje počet relací, příkazů a názvů, které jsou k dispozici pro použití aplikacemi. Tyto prostředky jsou k dispozici pro všechny aplikace založené na systému NetBIOS, které jsou spuštěny na stejném systému. Proto je možné, aby ostatní aplikace spotřebovávaly tyto prostředky dříve, než je produkt IBM MQ potřebuje získat. Administrátor sítě LAN by vám to měl být schopen vysvětlit.

Související pojmy

“Definování IBM MQ lokálního NetBIOS názvu” na stránce 255
Lokální název NetBIOS používaný procesy kanálu IBM MQ lze zadat třemi způsoby.

“Vytvoření omezení relací, příkazů a názvů správce front NetBIOS” na stránce 255
Omezení správce front pro relace, příkazy a názvy systému NetBIOS lze zadat dvěma způsoby.

“Zavedení čísla adaptéru LAN” na stránce 256
Aby kanály úspěšně fungovaly v rámci systému NetBIOS, musí být podpora adaptéru na obou koncích kompatibilní. Produkt IBM MQ vám umožňuje řídit volbu čísla adaptéru LAN (LANA) pomocí hodnoty AdapterNum v sekci NETBIOS vašeho souboru qm.ini a zadáním parametru **-a** v příkazu runmqlsr.

“Zahájení připojení NetBIOS” na stránce 256
Definování kroků potřebných k zahájení připojení.

“Definování cílového modulu listener pro připojení NetBIOS” na stránce 256
Definování kroků, které se mají provést na přijímacím konci připojení NetBIOS .

Windows *Definování IBM MQ lokálního NetBIOS názvu*

Lokální název NetBIOS používaný procesy kanálu IBM MQ lze zadat třemi způsoby.

V pořadí podle pořadí jsou tyto tři způsoby:

1. Hodnota uvedená v parametru **-l** příkazu **runmqlsr** , například:

   ```
   runmqlsr -t netbios -l my_station
   ```

2. Proměnná prostředí **MQNAME** s hodnotou zavedenou příkazem:

   ```
   SET MQNAME= my_station
   ```

   Příklad:

   ```
   SET MQNAME=CLIENT1
   ```

   Pro každý proces můžete nastavit hodnotu **MQNAME** . Případně jej můžete nastavit na úrovni systému v registru Windows .

   Používáte-li implementaci NetBIOS , která vyžaduje jedinečné názvy, musíte zadat příkaz **SET MQNAME** v každém okně, ve kterém je spuštěn proces IBM MQ . Hodnota **MQNAME** je libovolná, ale musí být jedinečná pro každý proces.

3. Sekce 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 byl každý název NetBIOS v síti jedinečný. Pokud tak neučiníte, může dojít k nepředvídatelným výsledkům. Máte-li problémy se zavedením kanálu NetBIOS a v protokolu chyb správce front jsou uvedeny chybové zprávy s návratovým kódem NetBIOS X'15 ', zkontrolujte použití názvů NetBIOS .
2. V systému Windowsnemůžete použít název počítače jako název NetBIOS , protože jej systém Windows již používá.
3. Inicializace kanálu odesilatele vyžaduje zadání názvu NetBIOS buď pomocí proměnné prostředí MQNAME, nebo pomocí LocalName v souboru qm.ini .

Windows *Vytvoření omezení relací, příkazů a názvů správce front NetBIOS*

Omezení správce front pro relace, příkazy a názvy systému NetBIOS lze zadat dvěma způsoby.

V pořadí podle pořadí jsou tyto způsoby:

1. Hodnoty zadané v příkazu RUNMQLSR:

```
-s Sessions
-e Names
-o Commands
```

   Není-li v příkazu zadán operand -m, platí tyto hodnoty pouze pro výchozího správce front.
2. Sekce NETBIOS v konfiguračním souboru správce front qm.ini. Příklad:

```
NETBIOS:

NumSess= Qmgr_max_sess
NumCmds= Qmgr_max_cmds
NumNames= Qmgr_max_names
```

Windows *Zavedení čísla adaptéru LAN*

Aby kanály úspěšně fungovaly v rámci systému NetBIOS, musí být podpora adaptéru na obou koncích kompatibilní. Produkt IBM MQ vám umožňuje řídit volbu 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, které používá systém IBM MQ pro připojení NetBIOS , je 0. Následujícím způsobem ověřte číslo používané ve vašem systému:

V systému Windowsnení možné zadávat dotazy na číslo adaptéru LAN přímo prostřednictvím operačního systému. Místo toho použijte LANACFG.EXE , k dispozici v adresáři Microsoft. Výstup nástroje zobrazuje čísla virtuálních adaptérů LAN a jejich efektivní vazby. Další informace o číslech adaptérů LAN viz Microsoft Článek znalostní báze 138037 *HOWTO: Použití čísel LANA ve 32bitovém prostředí*.

Zadejte správnou hodnotu v sekci NETBIOS konfiguračního souboru správce front qm.ini:

```
NETBIOS:
AdapterNum= n
```

kde n je správné číslo adaptéru LAN pro tento systém.

Windows *Zahájení připojení NetBIOS*

Definování kroků potřebných k zahájení připojení.

Chcete-li zahájit připojení, postupujte na odesílajícím konci takto:

1. Definujte název stanice NetBIOS pomocí hodnoty MQNAME nebo LocalName .
2. Ověřte číslo adaptéru LAN používané v systému a zadejte správný soubor pomocí parametru AdapterNum.
3. Do pole ConnectionName v definici kanálu zadejte název NetBIOS používaný cílovým programem modulu listener. V systému Windowsmusí být kanály NetBIOS spuštěny jako podprocesy. To provedete zadáním hodnoty MCATYPE (THREAD) v definici kanálu.

```
DEFINE CHANNEL (chname) CHLTYPE(SDR) +
TRPTYPE(NETBIOS) +
CONNAME(your_station) +
XMITQ(xmitq) +
MCATYPE(THREAD) +
REPLACE
```

Windows *Definování cílového modulu listener pro připojení NetBIOS*

Definování kroků, které se mají provést na přijímacím konci připojení NetBIOS .

Na konci příjmu postupujte takto:

1. Definujte název stanice NetBIOS pomocí hodnoty MQNAME nebo LocalName .
2. Ověřte číslo adaptéru LAN používané v systému a zadejte správný soubor pomocí parametru AdapterNum.
3. Definujte přijímací kanál:

```
DEFINE CHANNEL (chname) CHLTYPE(RCVR) +
TRPTYPE(NETBIOS) +
REPLACE
```

4. Spusťte program modulu listener IBM MQ , abyste ustanovili stanici a umožnili ji kontaktovat. Příklad:

```
RUNMQLSR -t NETBIOS -l your_station [-m qmgr]
```

   Tento příkaz zavede `your_station` jako stanici NetBIOS čekající na kontaktování. Název stanice NetBIOS musí být jedinečný v celé síti NetBIOS .

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu “Spuštění kanálů a modulů listener jako důvěryhodných aplikací” na stránce 239. Informace o důvěryhodných aplikacích naleznete v tématu Omezení důvěryhodných aplikací .

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

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

Pokud nezadáte název správce front, bude předpokládán výchozí správce front.

Linux AIX Nastavení komunikace na AIX and Linux

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby bylo připojení úspěšné, musí být definováno a k dispozici. Tento oddíl vysvětluje, jak to provést pomocí forem komunikace, které jsou k dispozici pro systémy IBM MQ for UNIX or Linux .

Než začnete

Pro vás může být užitečné, abyste se odkázali na následující části:

- AIX Příklad konfigurace- IBM MQ for AIX
- Linux Příklad konfigurace- IBM MQ pro Linux

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Informace o této úloze

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nezbytné, aby bylo připojení definováno a k dispozici. Tento oddíl vysvětluje, jak to provést.

Při nastavování komunikace pro systém IBM MQ na systému AIX and Linuxsi můžete vybrat z následujících typů komunikace:

- TCP/IP
- LU 6.2

Každá definice kanálu musí určovat pouze jeden atribut přenosového protokolu (typ přenosu). Správce front může použít jeden nebo více protokolů.

Pro systém IBM MQ MQI clientsmůže být užitečné mít alternativní kanály používající různé přenosové protokoly. Viz IBM MQ MQI clients.

Postup

Informace o nastavení komunikace pro systém AIX nebo Linux naleznete v podtématu pro zvolený typ komunikace:

- "Definování připojení TCP na systému AIX and Linux" na stránce 258
- "Definování připojení LU 6.2 na systému AIX and Linux" na stránce 262
- MQ Adv. MQ Adv. VUE "Definování připojení Aspera gateway na platformách Linux nebo Windows" na stránce 822

Související úlohy

"Monitorování a řízení kanálů na systému AIX, Linux, and Windows" na stránce 240
Pro aplikaci DQM je třeba vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Kanály můžete řídit pomocí příkazů, programů, IBM MQ Explorer, souborů pro definice kanálů a oblasti úložiště pro synchronizační informace.

"Konfigurace připojení mezi klientem a serverem" na stránce 14
Chcete-li konfigurovat komunikační spojení mezi produktem IBM MQ MQI clients a servery, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

"Nastavení komunikace na Windows" na stránce 250
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby bylo připojení úspěšné, musí být definováno a k dispozici. Tento oddíl vysvětluje, jak to provést pomocí forem komunikace, které jsou k dispozici pro systémy IBM MQ for Windows .

Související odkazy

"Jaký typ komunikace použít" na stránce 15
Různé platformy podporují různé komunikační protokoly. Vaše volba přenosového protokolu závisí na vaší kombinaci platformy IBM MQ MQI client a platformy serveru.

Linux AIX *Definování připojení TCP na systému AIX and Linux*

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

Než začnete

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Konec odesílání

Do pole Název připojení definice kanálu zadejte název hostitele nebo adresu TCP cílového počítače. Výchozí hodnota portu pro připojení je 1414. Číslo portu 1414 je přiřazeno autoritou Internet Assigned Numbers k IBM MQ.

Chcete-li použít jiné číslo portu než výchozí, změňte pole názvu připojení takto:

```
Connection Name REMHOST(1822)
```

kde REMHOST je název hostitele vzdáleného počítače a 1822 je požadované číslo portu. (Musí se jednat o port, na kterém naslouchá modul listener na přijímacím konci.)

Případně můžete číslo portu změnit jeho zadáním do konfiguračního souboru správce front (qm.ini):

```
TCP:
Port=1822
```

Další informace o hodnotách, které jste nastavili pomocí qm.ini, naleznete v části Sekce konfiguračního souboru pro distribuované fronty.

Příjem na TCP

Můžete použít buď modul listener TCP/IP, což je démon inet (inetd), nebo modul listener IBM MQ .

Některé distribuce systému Linux nyní používají démona xinetd (extended inet daemon) namísto démona inet. Další informace o použití rozšířeného démona inet v systému Linux viz Krok 2 Příklad: nastavení IBM MQ mezisložkové komunikace v systému Linux.

Související pojmy

"Použití modulu listener TCP/IP v systému AIX and Linux" na stránce 259
Chcete-li spustit kanály v systému AIX and Linux, je třeba upravit soubor `/etc/services` a soubor `inetd.conf` .

"Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému IBM MQ for Multiplatforms" na stránce 260
V protokolu TCP se s připojeními zachází jako s neúplnými, pokud mezi serverem a klientem nedojde k třícestnému navázání komunikace. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nevyřízené požadavky čekající na port TCP, aby mohl modul listener přijmout požadavek.

"Použití modulu listener IBM MQ" na stránce 261
Chcete-li spustit modul listener dodaný s produktem IBM MQ, který spouští nové kanály jako podprocesy, použijte příkaz `runmqlsr` .

"Použití volby TCP/IP SO_KEEPALIVE" na stránce 262
Na některých systémech AIX and Linux můžete definovat, jak dlouho TCP čeká, než zkontroluje, zda je připojení stále k dispozici, a jak často se pokusí o připojení znovu, pokud první kontrola selže. Jedná se buď o laditelný parametr jádra, nebo jej lze zadat na příkazový řádek.

Použití modulu listener TCP/IP v systému AIX and Linux

Chcete-li spustit kanály v systému AIX 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 superuživatel nebo uživatel root. Toto můžete změnit, ale musí odpovídat číslu portu uvedenému na odesílajícím konci.

   Přidejte do souboru následující parametr:

   ```
   MQSeries 1414/tcp
   ```

   kde 1414 je číslo portu požadované produktem IBM MQ. Číslo portu nesmí být vyšší než 65535.
2. Přidejte řádek do souboru `inetd.conf` pro volání programu amqcrsta, kde *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ :

   ```
   MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta
   [-m Queue_Man_Name]
   ```

Aktualizace jsou aktivní poté, co inetd znovu načte konfigurační soubory. Chcete-li tak učinit, zadejte následující příkazy z ID uživatele root:

- AIX V systému AIX:

```
refresh -s inetd
```

- Linux Na systémech Linux:

```
kill -1 process_number
```

Když program modulu listener spuštěný inetd zdědí národní prostředí od inetd, je možné, že MQMDE není respektován (sloučen) a je umístěn do fronty jako data zprávy. Chcete-li se ujistit, že je respektováno prostředí MQMDE, musíte správně nastavit národní prostředí. Národní prostředí nastavené pomocí inetd se nemusí shodovat s národním prostředím zvoleným pro jiná národní prostředí používaná procesy IBM MQ . Chcete-li nastavit národní prostředí, postupujte takto:

1. Vytvořte skript shellu, který nastaví proměnné národního prostředí LANG, LC_COLLATE, LC_CTYPE, LC_MONETARY, LC_NUMERIC, LC_TIME a LC_MESSAGES na národní prostředí použité pro jiný proces IBM MQ .
2. Ve stejném skriptu shellu volejte program modulu listener.
3. Upravte soubor `inetd.conf` tak, aby místo programu modulu listener volal skript shellu.

Na serveru je možné mít více než jednoho správce front. Musíte přidat řádek do každého ze dvou souborů pro každého ze správců front. Příklad:

```
MQSeries1   1414/tcp
MQSeries2   1822/tcp
```

```
MQSeries2 stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta -m QM2
```

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

Tím se vyhnete generování chybových zpráv, pokud existuje omezení počtu nevyřízených požadavků na připojení zařazených do fronty na jednom portu TCP. Informace o počtu nevyřízených požadavků na připojení viz “Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému IBM MQ for Multiplatforms” na stránce 260.

Multi *Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému IBM MQ for Multiplatforms*

V protokolu TCP se s připojeními zachází jako s neúplnými, pokud mezi serverem a klientem nedojde k třícestnému navázání komunikace. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nevyřízené požadavky čekající na port TCP, aby mohl modul listener přijmout požadavek.

Výchozí hodnoty seznamu nevyřízených požadavků modulu listener jsou uvedeny v souboru Tabulka 23 na stránce 260.

Tabulka 23. Maximální počet nevyřízených požadavků na připojení zařazených do fronty na portu TCP/IP

Platforma serveru	**Maximální počet požadavků na připojení**
AIX AIX	100
Linux Linux	100

Tabulka 23. Maximální počet nevyřízených požadavků na připojení zařazených do fronty na portu TCP/IP (pokračování)

Platforma serveru	Maximální počet požadavků na připojení
IBM i	255
Windows Server	100

Pokud nevyřízené požadavky dosáhnou hodnot uvedených v části Tabulka 23 na stránce 260, připojení TCP/IP bude odmítnuto a kanál nebude moci být spuštěn.

U kanálů MCA to má za následek, že kanál přejde do stavu RETRY a později se znovu pokusí o připojení.

Chcete-li se však vyhnout této chybě, můžete přidat položku do souboru `qm.ini` :

```
TCP:
ListenerBacklog = n
```

Tím se přepíše výchozí maximální počet nevyřízených požadavků (viz Tabulka 23 na stránce 260). pro modul listener TCP/IP.

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí hodnota. V případě potřeby lze tuto hodnotu použít, aby se zabránilo dosažení limitu připojení.

Chcete-li spustit modul listener s povolenou volbou `backlog` , postupujte takto:

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

Informace o příkazu **`runmqlsr`** viz runmqlsr. Informace o příkazu DEFINE LISTENER naleznete v tématu DEFINE LISTENER.

Související pojmy

“Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému z/OS” na stránce 973
Při příjmu v protokolu TCP/IP je nastaven maximální počet nevyřízených požadavků na připojení. Tyto neprovedené požadavky lze považovat za *nevyřízené* požadavky čekající na port TCP/IP, aby mohl modul listener přijmout požadavek.

Linux AIX *Použití modulu listener IBM MQ*

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

Příklad:

```
runmqlsr -t tcp [-m QMNAME] [-p 1822]
```

Hranaté závorky označují volitelné parametry; parametr `QMNAME` není pro výchozího správce front povinný a číslo portu není vyžadováno, pokud používáte výchozí hodnotu (1414). Číslo portu nesmí být vyšší než 65535.

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu “Spuštění kanálů a modulů listener jako důvěryhodných aplikací” na stránce 239. Informace o důvěryhodných aplikacích naleznete v tématu Omezení důvěryhodných aplikací .

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

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

Pokud nezadáte název správce front, bude předpokládán výchozí správce front.

Linux AIX *Použití volby TCP/IP SO_KEEPALIVE*

Na některých systémech AIX and Linux můžete definovat, jak dlouho TCP čeká, než zkontroluje, zda je připojení stále k dispozici, a jak často se pokusí o připojení znovu, pokud první kontrola selže. Jedná se buď o laditelný parametr jádra, nebo jej lze zadat na příkazový řádek.

Chcete-li použít volbu SO_KEEPALIVE (další informace viz “Kontrola, zda je druhý konec kanálu stále k dispozici” na stránce 225) Do konfiguračního souboru správce front (qm.ini) musíte přidat následující položku:

```
TCP:
KeepAlive=yes
```

Další informace naleznete v dokumentaci k systému AIX nebo Linux .

Linux AIX *Definování připojení LU 6.2 na systému AIX and Linux*

Architektura SNA musí být konfigurována tak, aby bylo možné mezi těmito dvěma počítači navázat konverzaci LU 6.2 .

Nejnovější informace o konfiguraci SNA přes TCP/IP naleznete v následující online dokumentaci IBM : Communications Server.

Architektura SNA musí být konfigurována tak, aby bylo možné mezi těmito dvěma systémy navázat konverzaci LU 6.2 .

Informace naleznete v příručce *Multiplatform APPC Configuration Guide* a v následující tabulce.

Tabulka 24. Nastavení v lokálním systému AIX nebo Linux pro vzdálenou platformu správce front

Vzdálená platforma	**TPNAME**	**TPPATH**
z/OS bez CICS	Stejné jako odpovídající TPName v postranních informacích o vzdáleném správci front.	-
z/OS použití CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-
IBM i	Stejná hodnota jako porovnávací hodnota v záznamu směrování v systému IBM i .	-
Systémy AIX and Linux	Stejné jako odpovídající TPName v postranních informacích o vzdáleném správci front.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo v vyvolatelném transakčním programu, který byl definován pomocí TpSetup na systému Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

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

Máte-li ve stejném počítači více než jednoho správce front, ujistěte se, že jsou názvy TPname v definicích kanálu jedinečné.

Související pojmy

“Odeslání ukončení na LU 6.2 na AIX and Linux” na stránce 263

V systémech AIX and Linux vytvořte objekt na straně rozhraní CPI-C (symbolické místo určení) a zadejte tento název do pole Název připojení v definici kanálu. Vytvořte také odkaz LU 6.2 na partnera.

"Příjem na logické jednotce 6.2 on AIX and Linux" na stránce 263
V systémech AIX and Linux vytvořte na konci příjmu připojení pro naslouchání, profil logického připojení LU 6.2 a profil TPN.

Linux AIX *Odeslání ukončení na LU 6.2 na AIX and Linux*
V systémech AIX and Linux vytvořte objekt na straně rozhraní CPI-C (symbolické místo určení) a zadejte tento název do pole Název připojení v definici kanálu. Vytvořte také odkaz LU 6.2 na partnera.

Do objektu na straně CPI-C zadejte jméno 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
```

Příkaz SECURITY PROGRAM se používá tam, kde jej podporuje rozhraní CPI-C, když se produkt IBM MQ pokusí vytvořit relaci SNA.

Linux AIX *Příjem na logické jednotce 6.2 on AIX and Linux*
V systémech AIX and Linux vytvořte na konci příjmu připojení pro naslouchání, profil logického připojení LU 6.2 a profil TPN.

V profilu TPN zadejte úplnou cestu ke spustitelnému souboru a název transakčního programu:

```
Full path to TPN executable    MQ_INSTALLATION_PATH/bin/amqcrs6a
Transaction Program name      recv
User ID                       0
```

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

V systémech, kde můžete nastavit ID uživatele, zadejte uživatele, který je členem skupiny mqm.

AIX V systémech AIXnastavte proměnné prostředí APPCTPN (název transakce) a APPCLLU (název lokální LU) (můžete použít konfigurační panely pro vyvolaný transakční program).

Může být nutné použít jiného správce front než výchozího správce front. Pokud ano, definujte příkazový soubor, který volá:

```
amqcrs6a -m Queue_Man_Name
```

pak zavolejte příkazový soubor.

IBM i Monitorování a řízení kanálů na systému IBM i

Pomocí panelů a příkazů DQM můžete vytvářet, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení s kompatibilními vzdálenými správci front.

Informace o této úloze

Následující seznam obsahuje stručný popis komponent funkce řízení kanálu:

- Definice kanálů jsou uchovávány jako objekty správce front.
- Příkazy kanálu jsou podmnožinou sady příkazů IBM MQ for IBM i .

  Pomocí příkazu GO CMDMQM zobrazte úplnou sadu příkazů IBM MQ for IBM i .
- Panely definic kanálů nebo příkazy se používají k:

  - Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálů.
  - Spuštění a zastavení kanálů, příkaz ping, resetování pořadových čísel kanálů a vyřešení nejistých zpráv v případě, že odkazy nelze znovu navázat.
  - Zobrazit informace o stavu kanálů
- Kanály lze také spravovat pomocí MQSC
- Kanály lze také spravovat pomocí Průzkumníka IBM MQ .
- Pořadová čísla a *logické pracovní jednotky (LUW)* identifikátory jsou uloženy v synchronizačním souboru a používají se pro účely synchronizace kanálu.

Příkazy a panely můžete použít k: definování kanálů zpráv a přidružených objektů a k monitorování a řízení kanálů zpráv. Pomocí klávesy F4=Prompt můžete zadat příslušného správce front. Pokud výzvu nepoužijete, předpokládá se výchozí správce front. Pomocí volby F4=Promptse zobrazí další panel, kde můžete zadat příslušný název správce front a někdy i jiná data.

Objekty, které potřebujete definovat pomocí panelů, jsou:

- Přenosové fronty
- Definice vzdálené fronty
- Definice aliasů správce front
- Definice aliasu fronty pro odpověď
- Lokální fronty pro odpovědi
- Definice kanálů zpráv

Další informace o koncepcích, které se podílejí na použití těchto objektů, viz “Konfigurace distribuovaných front” na stránce 189.

Kanály musí být zcela definovány a jejich přidružené objekty musí existovat a být k dispozici pro použití, než bude možné kanál spustit.

Kromě toho musí být před spuštěním kanálu definováno a k dispozici konkrétní komunikační propojení pro každý kanál. Popis toho, jak jsou definovány spoje LU 6.2 a TCP/IP, naleznete v konkrétní komunikační příručce pro vaši instalaci.

Procedura

- Další informace o vytváření a práci s objekty viz:
  - “Vytváření objektů v systému IBM i” na stránce 265
  - “Vytvoření kanálu v systému IBM i” na stránce 265
  - “Spuštění kanálu v systému IBM i” na stránce 267
  - “Výběr kanálu v systému IBM i” na stránce 267
  - “Procházení kanálu v systému IBM i” na stránce 268
  - “Přejmenování kanálu v systému IBM i” na stránce 269
  - “Práce se stavem kanálu na systému IBM i” na stránce 270
  - “Volby funkce Work-with-channel na systému IBM i” na stránce 270

Související pojmy

“Nastavení komunikace pro IBM i” na stránce 276
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Má-li být připojení úspěšné, musí být definováno a k dispozici.

Související úlohy

“Konfigurace připojení mezi klientem a serverem” na stránce 14
Chcete-li konfigurovat komunikační spojení mezi produktem IBM MQ MQI clients a servery, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

Související odkazy
Příklad konfigurace- IBM MQ for IBM i
Příklad plánování kanálu zpráv pro IBM MQ for IBM i
IBM MQ for IBM i CL příkazy

IBM i Vytváření objektů v systému IBM i

K vytvoření objektů front a aliasů můžete použít příkaz CRTMQMQ.

Můžete vytvořit objekty front a aliasů, například: přenosové fronty, definice vzdálených front, definice aliasů správců front, definice aliasů front pro odpovědi a lokální fronty pro odpovědi.

Seznam výchozích objektů viz Systémové a výchozí objekty.

IBM i Vytvoření kanálu v systému IBM i

Kanál můžete vytvořit z panelu Vytvořit kanál nebo pomocí příkazu CRTMQMCHL na příkazovém řádku.

Chcete-li vytvořit kanál, postupujte takto:

1. Použijte hodnotu F6 z panelu Práce s kanály MQM (WRKMQMCHL).

   Případně použijte příkaz CRTMQMCHL z příkazového řádku.

   V obou případech se zobrazí panel Vytvořit kanál. Typ:

   - Název kanálu v poskytnutém poli
   - Typ kanálu pro tento konec odkazu
2. Stiskněte klávesu Enter.

Poznámka: Všechny kanály v síti musíte pojmenovat jedinečně. Jak ukazuje Diagram sítě zobrazující všechny kanály, včetně názvů zdrojového a cílového správce front v názvu kanálu je vhodný způsob, jak to provést.

Vaše položky jsou ověřeny a chyby jsou ohlášeny okamžitě. Opravte všechny chyby a pokračujte.

Zobrazí se panel s příslušným nastavením kanálu pro zvolený typ kanálu. Vyplňte pole s informacemi, které jste shromáždili dříve. Chcete-li vytvořit kanál, stiskněte klávesu Enter.

Je vám poskytnuta pomoc při rozhodování o obsahu různých polí v popisech panelů definice kanálu na panelech nápovědy a v části Atributy kanálu.

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Channel name . . . . . > CHANNAME_____________
Channel type . . . . . > *SDR__    *RCVR, *SDR, *SVR, *RQSTR...
Message Queue Manager name     *DFT_____________________________
_____
Replace . . . . . .  *NO_     *NO, *YES
Transport type . . . . . .  *TCP____    *LU62, *TCP, *SYSDFTCHL
Text 'description' . . . . . > 'Example Channel Definition'_____________
_____________________________________
Connection name . . . . . .  *SYSDFTCHL_____________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________
More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 25. Vytvořit kanál (1)

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Transmission queue . . . . . .  'TRANSMISSION_QUEUE_NAME'_____________________
_____________________
Message channel agent . . . . .  *NONE______  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
Message channel agent user ID .  *SYSDFTCHL__ Character value...
Coded Character Set Identifier   *SYSDFTCHL__ 0-9999, *SYSDFTCHL
Batch size . . . . . .  50_________  1-9999, *SYSDFTCHL
Disconnect interval . . . . . .  6000_______  1-999999, *SYSDFTCHL
Short retry interval . . . . . .  60_________  0-999999999, *SYSDFTCHL
Short retry count . . . . . .  10_________  0-999999999, *SYSDFTCHL
Long retry interval . . . . . .  1200_______  0-999999999, *SYSDFTCHL
Long retry count . . . . . .  999999999__  0-999999999, *SYSDFTCHL
Security exit . . . . . .  *NONE_____  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
Security exit user data . . . .  *SYSDFTCHL_____________________

More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 26. Vytvořit kanál (2)

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Send exit . . . . . .  *NONE______  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________ Name
+ for more values   __________
Send exit user data . . . . . .  _________________________________
+ for more values  _________________________________
Receive exit . . . . . .  *NONE_____  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
+ for more values  __________
__________
Receive exit user data . . . . .  _________________________________
+ for more values  _________________________________
Message exit . . . . . .  *NONE_____  Name, *SYSDFTCHL, *NONE
Library . . . . . .  __________  Name
+ for more values  __________
__________
More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 27. Vytvořit kanál (3)

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Message exit user data . . . . .  _________________________________
+ for more values  _________________________________
Convert message . . . . . .  *SYSDFTCHL_  *YES, *NO, *SYSDFTCHL
Sequence number wrap . . . . . .  999999999__  100-999999999, *SYSDFTCHL
Maximum message length . . . . .  4194304____  0-4194304, *SYSDFTCHL
Heartbeat interval . . . . . .  300________  0-999999999, *SYSDFTCHL
Non Persistent Message Speed . .  *FAST_____  *FAST, *NORMAL, *SYSDFTCHL
Password . . . . . .  *SYSDFTCHL_  Character value, *BLANK...
Task User Profile . . . . . .  *SYSDFTCHL_  Character value, *BLANK...
Transaction Program Name . . . .  *SYSDFTCHL



Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 28. Vytvořit kanál (4)

IBM i Spuštění kanálu v systému IBM i

Kanál můžete spustit z panelu Práce s kanály nebo pomocí příkazu STRMQMCHL na příkazovém řádku.

Listenery jsou platné pouze pro TCP. Pro listenery SNA musíte nakonfigurovat komunikační subsystém.

Aby mohly aplikace vyměňovat zprávy, musíte spustit program modulu listener pro příchozí připojení pomocí příkazu STRMQMLSR.

V případě odchozích připojení musíte kanál spustit jedním z následujících způsobů:

1. Pomocí CL příkazu STRMQMCHL, který určuje název kanálu, spusťte kanál jako proces nebo podproces v závislosti na parametru MCATYPE. (Pokud jsou kanály spouštěny jako podprocesy, jedná se o podprocesy inicializátoru kanálu.)

   ```
   STRMQMCHL CHLNAME(QM1.TO.QM2) MQNAME(MYQMGR)
   ```

2. Ke spuštění kanálu použijte iniciátor kanálu. Při spuštění správce front je automaticky spuštěn jeden inicializátor kanálu. Toto automatické spuštění lze odstranit změnou sekce chinit v souboru qm.ini pro tohoto správce front.
3. Použijte příkaz WRKMQMCHL k zahájení panelu Práce s kanály a zvolte volbu 14 ke spuštění kanálu.

IBM i Výběr kanálu v systému IBM i

Kanál můžete vybrat z panelu Práce s kanály.

Chcete-li vybrat kanál, použijte příkaz WRKMQMCHL k zahájení práce na panelu Práce s kanály:

1. Přesuňte kurzor na pole volby přidružené k požadovanému názvu kanálu.
2. Zadejte číslo volby.
3. Stisknutím klávesy Enter aktivujte svou volbu.

Vyberete-li více než jeden kanál, budou volby postupně aktivovány.

```
Work with MQM Channels

Queue Manager Name . . :  CNX

Type options, press Enter.
2=Change  3=Copy  4=Delete  5=Display  8=Work with Status  13=Ping
14=Start  15=End  16=Reset  17=Resolve

Opt   Name           Type    Transport   Status
CHLNIC          *RCVR    *TCP     INACTIVE
CORSAIR.TO.MUSTANG    *SDR    *LU62    INACTIVE
FV.CHANNEL.MC.DJE1    *RCVR    *TCP     INACTIVE
FV.CHANNEL.MC.DJE2    *SDR    *TCP     INACTIVE
FV.CHANNEL.MC.DJE3    *RQSTR   *TCP     INACTIVE
FV.CHANNEL.MC.DJE4    *SVR    *TCP     INACTIVE
FV.CHANNEL.PETER     *RCVR    *TCP     INACTIVE
FV.CHANNEL.PETER.LU   *RCVR    *LU62    INACTIVE
FV.CHANNEL.PETER.LU1   *RCVR    *LU62    INACTIVE
More...
Parameters or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Create  F9=Retrieve  F12=Cancel
F21=Print
```

Obrázek 29. Práce s kanály

IBM i Procházení kanálu v systému IBM i

Kanál můžete procházet z panelu Zobrazit kanál nebo pomocí příkazu DSPMQMCHL na příkazovém řádku.

Chcete-li procházet nastavení kanálu, použijte příkaz WRKMQMCHL k zahájení na panelu Zobrazit kanál:

1. Zadejte volbu 5 (Zobrazení) pro požadovaný název kanálu.
2. Stisknutím klávesy Enter aktivujte svou volbu.

Vyberete-li více než jeden kanál, budou zobrazeny postupně.

Případně můžete použít příkaz DSPMQMCHL z příkazového řádku.

To má za následek zobrazení příslušného panelu Zobrazit kanál s podrobnostmi o aktuálním nastavení kanálu. Pole jsou popsána v části Atributy kanálu.

```
Display MQM Channel

Channel name . . . . . :  ST.JST.2TO1
Queue Manager Name . . . . . :  QMREL
Channel type . . . . . :  *SDR
Transport type . . . . . :  *TCP
Text 'description' . . . . . :  John's sender to WINSDOA1

Connection name . . . . . :  MUSTANG


Transmission queue . . . . . :  WINSDOA1

Message channel agent . . . . :
Library . . . . . :
Message channel agent user ID :  *NONE
Batch interval . . . . . :  0
Batch size . . . . . :  50
Disconnect interval . . . . . :  6000



F3=Exit  F12=Cancel  F21=Print
```

Obrázek 30. Zobrazení kanálu TCP/IP (1)

```
Display MQM Channel

Short retry interval . . . . . :  60
Short retry count . . . . . :  10
Long retry interval . . . . . :  6000
Long retry count . . . . . :  10
Security exit . . . . . :
Library . . . . . :
Security exit user data . . . :
Send exit . . . . . :
Library . . . . . :
Send exit user data . . . . . :
Receive exit . . . . . :
Library . . . . . :
Receive exit user data . . . . :
Message exit . . . . . :
Library . . . . . :
Message exit user data . . . . :
More...


F3=Exit  F12=Cancel  F21=Print
```

Obrázek 31. Zobrazení kanálu TCP/IP (2)

```
Display MQM Channel

Sequence number wrap . . . . . :  999999999
Maximum message length . . . . :  10000
Convert message . . . . . :  *NO
Heartbeat interval . . . . . :  300
Nonpersistent message speed . .  *FAST









Bottom



F3=Exit  F12=Cancel  F21=Print
```

Obrázek 32. Zobrazení kanálu TCP/IP (3)

IBM i Přejmenování kanálu v systému IBM i

Kanál můžete přejmenovat z panelu Práce s kanály.

Chcete-li přejmenovat kanál zpráv, začněte na panelu Práce s kanály:

1. Ukončete kanál.
2. Pomocí volby 3 (Kopírovat) vytvořte duplikát s novým názvem.
3. Pomocí volby 5 (Zobrazení) zkontrolujte, zda byla správně vytvořena.
4. K odstranění původního kanálu použijte volbu 4 (Odstranit).

Pokud se rozhodnete přejmenovat kanál zpráv, ujistěte se, že oba konce kanálu jsou přejmenovány současně.

IBM i Práce se stavem kanálu na systému IBM i

Se stavem kanálu můžete pracovat na panelu Práce se stavem kanálu.

Pomocí příkazu WRKMQMCHST zobrazte první ze sady panelů, které zobrazují stav vašich kanálů. Můžete zobrazit stavové panely v pořadí, když vyberete Změnit zobrazení (F11).

Alternativně výběrem volby 8 (Práce se stavem) na panelu Práce s kanály MQM také zobrazíte první stavový panel.

```
MQSeries Work with Channel Status

Type options, press Enter.
5=Display  13=Ping  14=Start  15=End  16=Reset  17=Resolve


Opt Name          Connection      Indoubt   Last Seq
CARTS_CORSAIR_CHAN  GBIBMIYA.WINSDOA1    NO        1
CHLNIC        9.20.2.213       NO        3
FV.CHANNEL.PETER2   9.20.2.213       NO      6225
JST.1.2        9.20.2.201       NO       28
MP_MUST_TO_CORS    9.20.2.213       NO       100
MUSTANG.TO.CORSAIR  GBIBMIYA.WINSDOA1    NO       10
MP_CORS_TO_MUST    9.20.2.213       NO       101
JST.2.3        9.5.7.126        NO       32
PF_WINSDOA1_LU62   GBIBMIYA.IYA80020    NO       54
PF_WINSDOA1_LU62   GBIBMIYA.WINSDOA1    NO       500
ST.JCW.EXIT.2TO1.CHL 9.20.2.213       NO       216

Bottom
Parameters or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Create  F9=Retrieve  F11=Change view
F12=Cancel  F21=Print
```

Obrázek 33. První ze sady stavových panelů kanálu

Na panelu Práce se stavem kanálu jsou k dispozici následující volby:

Volba nabídky	Popis
5=Display	Zobrazí nastavení kanálu.
13=Ping	Zahájí akci příkazu ping, je-li to vhodné.
14=Start	Spustí kanál.
15=End	Zastaví kanál.
16=Reset	Resetuje pořadové číslo kanálu.
17=Resolve	Řeší nejistou situaci kanálu ručně.

IBM i Volby funkce Work-with-channel na systému IBM i

Panel Práce s kanály je dosažen příkazem WRKMQMCHL a umožňuje vám monitorovat stav všech vypsaných kanálů a vydávat příkazy pro vybrané kanály.

Na panelu Práce s kanálem jsou k dispozici následující volby:

Volba nabídky	Popis
“2=Change” na stránce 271	Změní atributy kanálu.
“3=Copy” na stránce 271	Zkopíruje atributy kanálu do nového kanálu.

Volba nabídky	Popis
“4=Delete” na stránce 272	Odstraní kanál.
“5=Display” na stránce 272	Zobrazí aktuální nastavení kanálu.
“6=Create” na stránce 272	Zobrazí panel Vytvořit kanál.
“8=Work se stavem” na stránce 272	Zobrazí stavové panely kanálu.
“13=Ping” na stránce 273	Spustí službu Ping, která otestuje připojení k sousednímu systému výměnou pevné datové zprávy se vzdáleným koncem.
“14=Start” na stránce 273	Spustí vybraný kanál nebo resetuje zakázaný přijímací kanál.
“15=End” na stránce 274	Požaduje ukončení kanálu.
“16=Reset” na stránce 275	Požádá kanál o resetování pořadových čísel na tomto konci linky. Čísla musí být stejná na obou koncích, aby se kanál spustil.
“17=Resolve” na stránce 275	Požádá kanál o vyřešení nejistých zpráv bez navázání připojení k druhému konci.
“18=Zobrazení oprávnění” na stránce 275	Zobrazí oprávnění k objektu IBM MQ
“19=Udělení oprávnění” na stránce 276	Uděluje oprávnění k objektu IBM MQ
“20=Odvolání oprávnění” na stránce 276	Odvolá oprávnění k objektu IBM MQ
“21=Zotavit objekt” na stránce 276	Obnoví objekt IBM MQ
“22=Záznam obrazu” na stránce 276	Obrázek objektu záznamů IBM MQ

IBM i *2=Change*

Pomocí volby Změnit změňte existující definici kanálu.

Volba Změna nebo příkaz CHGMQMCHL změní existující definici kanálu s výjimkou názvu kanálu. Zapište pole, která se mají změnit na panelu definice kanálu, a pak uložte aktualizovanou definici stisknutím klávesy Enter.

IBM i *3=Copy*

Pomocí volby Kopírovat zkopírujte existující kanál.

Volba Kopírovat používá příkaz CPYMQMCHL ke kopírování existujícího kanálu. Panel Kopírovat umožňuje definovat nový název kanálu. Musíte však omezit znaky použité na ty znaky, které jsou platné pro názvy objektů IBM i ; viz Administrace IBM MQ for IBM i.

Stiskněte klávesu Enter na panelu Kopírovat, abyste zobrazili podrobnosti aktuálního nastavení. Můžete změnit libovolné nové nastavení kanálu. Uložte novou definici kanálu stisknutím klávesy Enter.

IBM i 4=Delete

Chcete-li odstranit vybraný kanál, použijte volbu Odstranit.

Zobrazí se panel pro potvrzení nebo zrušení vašeho požadavku.

IBM i 5=Display

Chcete-li zobrazit aktuální definice kanálu, použijte volbu Zobrazit.

Tato volba zobrazí panel s poli zobrazujícími aktuální hodnoty parametrů a chráněnými proti vstupu uživatele.

IBM i 6=Create

Pomocí volby Vytvořit zobrazte panel Vytvořit kanál.

Použijte volbu Vytvořit nebo zadejte příkaz CRTMQMCHL z příkazového řádku, abyste získali panel Vytvořit kanál. Existují příklady panelů Vytvořit kanál, které začínají na adrese Obrázek 25 na stránce 265.

Pomocí tohoto panelu vytvoříte definici kanálu z obrazovky polí vyplněných výchozími hodnotami dodanými produktem IBM MQ for IBM i. Zadejte název kanálu, vyberte typ kanálu, který vytváříte, a komunikační metodu, která se má použít.

Po stisknutí klávesy Enter se zobrazí panel. Zapište informace do všech požadovaných polí v tomto panelu a zbývajících panelech a pak uložte definici stisknutím klávesy Enter.

Název kanálu musí být na obou koncích kanálu stejný a jedinečný v rámci sítě. Avšak musíte omezit znaky použité na ty znaky, které jsou platné pro názvy objektů IBM MQ for IBM i .

Všechny panely mají výchozí hodnoty dodané produktem IBM MQ for IBM i pro některá pole. Tyto hodnoty můžete upravit, nebo je můžete změnit při vytváření nebo kopírování kanálů. Chcete-li upravit hodnoty, prohlédněte si téma *IBM MQ for IBM i Administrace systému*.

Můžete vytvořit vlastní sadu výchozích hodnot kanálu tak, že nastavíte fiktivní kanály s požadovanými výchozími hodnotami pro každý typ kanálu a zkopírujete je pokaždé, když budete chtít vytvořit nové definice kanálu.

Související odkazy

Atributy kanálu

IBM i 8=Work se stavem

Chcete-li zobrazit podrobné informace o stavu kanálu, použijte volbu Práce se stavem.

Sloupec stavu informuje o tom, zda je kanál aktivní nebo neaktivní, a je zobrazen nepřetržitě na panelu Práce s kanály MQM. Použijte volbu 8 (Práce se stavem), abyste zobrazili další informace o stavu. Alternativně lze tyto informace zobrazit z příkazového řádku pomocí příkazu WRKMQMCHST. Viz “Práce se stavem kanálu na systému IBM i” na stránce 270.

- Název kanálu
- Typ kanálu
- Stav kanálu
- Instance kanálu
- Vzdálený správce front
- Jméno přenosové fronty
- Název komunikačního připojení
- Nejistý stav kanálu
- Poslední pořadové číslo
- Počet nejistých zpráv
- Pořadové číslo, které vyvolává pochybnosti
- Počet zpráv v přenosové frontě

- Identifikátor logické pracovní jednotky
- Identifikátor neověřené logické pracovní jednotky
- Dílčí stav kanálu
- Monitorování kanálů
- Komprese záhlaví
- Komprese zpráv
- Indikátor času komprese
- Indikátor rychlosti komprese
- Indikátor doby přenosové fronty
- Indikátor času sítě
- Indikátor času ukončení
- Indikátor velikosti dávky
- Aktuální sdílené konverzace
- Maximální počet sdílených konverzací

IBM i *13=Ping*

Použijte volbu Ping k výměně pevné datové zprávy se vzdáleným koncem.

Úspěšný příkaz ping systému IBM MQ dává supervizorovi systému určitou jistotu, že kanál je k dispozici a funguje.

Příkaz ping nezahrnuje použití přenosových front a cílových front. Používá definice kanálů, související komunikační spojení a nastavení sítě.

Je k dispozici pouze z kanálů odesilatele a serveru. Odpovídající kanál je spuštěn na vzdálené straně propojení a provádí vyjednávání parametrů spuštění. Chyby jsou upozorněny normálně.

Výsledek výměny zpráv je uveden na panelu Ping a je vráceným textem zprávy spolu s časem odeslání zprávy a časem přijetí odpovědi.

Příkaz ping s LU 6.2

Když je příkaz ping vyvolán v produktu IBM MQ for IBM i, je spuštěn s ID uživatele požadujícího funkci, zatímco normální způsob spuštění programu kanálu je pro ID uživatele QMQM, které má být použito pro programy kanálu. ID uživatele směřuje na přijímající stranu a musí být platné na přijímacím konci, aby byla konverzace LU 6.2 přidělena.

IBM i *14=Start*

Chcete-li spustit kanál ručně, použijte volbu Spustit.

Volba Start je k dispozici pro kanály odesilatele, serveru a žadatele. Není nutné, aby byl kanál nastaven se spouštěcím správcem front.

Volba Start se také používá pro kanály příjemce, připojení serveru, odesílatele klastru a příjemce klastru. Spuštění přijímacího kanálu, který je ve stavu ZASTAVENO, znamená, že jej lze spustit ze vzdáleného kanálu.

Po spuštění odesílající agent MCA přečte soubor definice kanálu a otevře přenosovou frontu. Je vydána spouštěcí posloupnost kanálu, která vzdáleně spustí odpovídající MCA kanálu příjemce nebo serveru. Po spuštění odesilatel a procesy serveru čekají na zprávy přicházející do přenosové fronty a odesílají je tak, jak dorazí.

Když použijete spouštění, musíte spustit souvisle spuštěný proces spouštěče, abyste monitorovali inicializační frontu. Pro spuštění procesu lze použít příkaz STRMQMCHLI.

Na vzdáleném konci kanálu může být přijímací proces spuštěn jako odpověď na spuštění kanálu z odesílajícího konce. Způsob, jak to udělat, se liší pro kanály připojené pomocí LU 6.2 a TCP/IP:

- Připojené kanály LU 6.2 nevyžadují na přijímacím konci kanálu žádnou explicitní akci.
- Kanály připojené pomocí protokolu TCP vyžadují, aby proces modulu listener běžel nepřetržitě. Tento proces čeká na požadavky na spuštění kanálu ze vzdáleného konce odkazu a spustí proces definovaný v definicích kanálu pro dané připojení.

  Když je vzdálený systém IBM i, můžete použít příkaz STRMQMLSR.

Použití volby Start vždy způsobí opětovnou synchronizaci kanálu, je-li to nutné.

Pro začátek uspět:

- Definice kanálů, lokální a vzdálené musí existovat. Pokud neexistuje odpovídající definice kanálu pro příjemce nebo kanál připojení serveru, automaticky se vytvoří výchozí, pokud je kanál automaticky definován. Viz Uživatelský program automatické definice kanálu.
- Přenosová fronta musí existovat, musí být povolena pro modul GETs a nesmí ji používat žádné jiné kanály.
- Lokální a vzdálené MCA musí existovat.
- Komunikační spojení musí být k dispozici.
- Správci front musí být spuštěni, lokální a vzdálení.
- Kanál zpráv musí být neaktivní.

Chcete-li přenášet zprávy, musí existovat vzdálené fronty a definice vzdálených front.

Na panel se vrátí zpráva potvrzující, že požadavek na spuštění kanálu byl přijat. Chcete-li potvrdit, že proces spuštění proběhl úspěšně, zkontrolujte systémový protokol, nebo stiskněte klávesu F5 (obnovte obrazovku).

IBM i *15=End*

Pomocí funkce End zastavíte aktivitu kanálu.

Volbu End použijte k vyžádání kanálu pro zastavení aktivity. Kanál neodesílá žádné další zprávy.

Před stisknutím klávesy Enter vyberte volbu F4 , abyste zvolili, zda se kanál stane ZASTAVENÝ nebo NEAKTIVNÍ, a zda se má zastavit kanál pomocí příkazu CONTROLLED nebo IMMEDIATE stop. Zastavený kanál musí být restartován operátorem, aby se znovu stal aktivním. Lze spustit neaktivní kanál.

Zastavit okamžitě

Chcete-li zastavit kanál bez dokončení jakékoli jednotky práce, použijte příkaz Zastavit okamžitě.

Tato volba ukončí proces kanálu. Výsledkem je, že kanál nedokončí zpracování aktuální dávky zpráv, a proto nemůže nechat kanál v nejistém stavu. Obecně je pro operátory lepší použít volbu řízeného zastavení.

Zastavit řízené

Pomocí příkazu Stop controlled zastavíte kanál na konci aktuální jednotky práce.

Tato volba požaduje, aby byl kanál řádně ukončen; aktuální dávka zpráv je dokončena a procedura synchronizačního bodu je provedena s druhým koncem kanálu.

Restartování zastavených kanálů

Když kanál přejde do stavu ZASTAVENO, musíte jej restartovat ručně. Kanál můžete restartovat následujícími způsoby:

- Pomocí příkazu **START CHANNEL** MQSC.
- Pomocí příkazu **Start Channel** PCF.

- Pomocí konzoly IBM MQ Explorer.
- z/OS V systému z/OSpomocí panelu Spustit kanál.
- IBM i V systému IBM ipomocí příkazu **STRMQMCHL CL** nebo volby **START** na panelu WRKMQMCHL.

V případě kanálů odesilatele nebo serveru byla při vstupu kanálu do stavu STOPPED (zastaveno) přidružená přenosová fronta nastavena na hodnotu GET (DISABLED) a spouštění bylo nastaveno na hodnotu GET (DISABLED). Když je přijat požadavek na spuštění, tyto atributy se automaticky vynulují.

z/OS Pokud se iniciátor kanálu zastaví v době, kdy je kanál ve stavu RETRYING nebo STOPPED, stav kanálu se při restartování inicializátoru kanálu zapamatuje. Avšak stav kanálu pro typ kanálu SVRCONN je resetován, pokud se iniciátor kanálu zastaví, když je kanál ve stavu ZASTAVENO.

Multi Pokud se správce front zastaví v době, kdy je kanál ve stavu RETRYING nebo STOPPED, stav kanálu se při restartování správce front zapamatuje. Od roku IBM MQ 8.0 to platí i pro kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

IBM i *16=Reset*

Chcete-li vynutit novou posloupnost zpráv, použijte volbu Resetovat.

Volba Reset změní pořadové číslo zprávy. Používejte jej opatrně a pouze poté, co jste použili volbu Vyřešit, abyste vyřešili jakékoli neověřené situace. Tato volba je k dispozici pouze u kanálu odesilatele nebo serveru. První zpráva spustí novou posloupnost při příštím spuštění kanálu.

IBM i *17=Resolve*

Pomocí volby Vyřešit vynutíte lokální potvrzení nebo vrácení nejistých zpráv zadržených v přenosové frontě.

Volbu Vyřešit použijte, když jsou zprávy zadrženy v nejistém stavu odesílatelem nebo serverem, například proto, že jeden konec odkazu byl ukončen a není možné, aby se obnovily. Volba Resolve přijímá jeden ze dvou parametrů: BACKOUT nebo COMMIT. Volba Backout obnoví zprávy do přenosové fronty, zatímco volba Commit je vyřadí.

Program kanálu se nepokouší ustanovit relaci s partnerem. Místo toho určuje identifikátor logické pracovní jednotky (LUWID), který představuje neověřené zprávy. Poté vydá, jak bylo požadováno, buď:

- BACKOUT pro obnovu zpráv do přenosové fronty; nebo
- COMMIT pro odstranění zpráv z přenosové fronty.

Aby usnesení uspělo:

- Kanál musí být neaktivní
- Kanál musí být nejistý
- Typ kanálu musí být odesilatel nebo server.
- Lokální definice kanálu musí existovat.
- Správce front musí být spuštěn, lokální

IBM i *18=Zobrazení oprávnění*

Použijte volbu Zobrazit oprávnění k zobrazení akcí, které má uživatel oprávnění provádět na určitém objektu IBM MQ .

Pro vybraný objekt a uživatele příkaz DSPMQAUT zobrazuje oprávnění, která má uživatel k provedení akcí s objektem IBM MQ . Pokud je uživatel členem více skupin, příkaz zobrazí kombinovanou autorizaci všech skupin k objektu.

IBM i 19=Udělení oprávnění

Pomocí volby Udělit oprávnění udělte oprávnění k provádění akcí na objektech IBM MQ jinému uživateli nebo skupině uživatelů.

Příkaz GRTMQMAUT je k dispozici pouze pro uživatele ve skupině QMQMADM. Uživatel v QMQMADM uděluje oprávnění ostatním uživatelům provádět akce s objekty IBM MQ jmenovanými v příkazu buď identifikací uživatelů podle jména, nebo udělením oprávnění všem uživatelům v *PUBLIC.

IBM i 20=Odvolání oprávnění

Oprávnění k odebrání oprávnění k provádění akcí s objekty od uživatelů použijte k odebrání oprávnění.

Příkaz RVKMQMAUT je k dispozici pouze uživatelům ve skupině QMQMADM. Uživatel ve skupině QMQMADM odebere oprávnění od ostatních uživatelů k provádění akcí s objekty IBM MQ jmenovanými v příkazu buď identifikací uživatelů podle jména, nebo odvoláním oprávnění od všech uživatelů v *PUBLIC.

IBM i 21=Zotavit objekt

Použijte volbu Obnovit objekt k obnově poškozených objektů z informací uložených v žurnálech IBM MQ .

Obnova objektu používá příkaz Znovu vytvořit objekt produktu MQ (RCRMQMOBJ) k obnově všech objektů, které jsou poškozeny a jsou uvedeny v příkazu. Pokud objekt není poškozen, neprovede se na něm žádná akce.

IBM i 22=Záznam obrazu

Obraz záznamu použijte ke snížení počtu žurnálových zásobníků požadovaných pro obnovu sady objektů a k minimalizaci doby obnovy.

Příkaz RCDMQMIMG přebírá kontrolní bod pro všechny objekty vybrané v příkazu. Synchronizuje aktuální hodnoty objektů v integrovaném systému souborů (IFS) s pozdějšími informacemi o objektech, jako např. MQPUTs a MQGETs, zaznamenanými v žurnálových zásobnících.

Když příkaz dokončí objekty v IFS, jsou aktuální a tyto žurnálové zásobníky již nemusí být přítomny pro obnovu objektů. Odpojené žurnálové zásobníky mohou být odpojeny (pokud nejsou přítomny pro obnovu jiných objektů).

IBM i Nastavení komunikace pro IBM i

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Má-li být připojení úspěšné, musí být definováno a k dispozici.

DQM je služba vzdáleného řízení front pro produkt IBM MQ for IBM i. Poskytuje programy pro řízení kanálů pro správce front IBM MQ for IBM i , který tvoří rozhraní pro komunikační propojení, které jsou řízeny systémovým operátorem.

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Má-li být připojení úspěšné, musí být definováno a k dispozici. Tento oddíl vysvětluje, jak zajistit, aby bylo připojení definováno a k dispozici.

Před spuštěním kanálu musí být přenosová fronta definována tak, jak je popsáno v této části, a musí být zahrnuta v definici kanálu zpráv.

Můžete si vybrat jednu z následujících dvou forem komunikace mezi systémy IBM MQ for IBM i :

- “Definování připojení TCP na systému IBM i” na stránce 277

  Pro protokol TCP lze použít adresu hostitele a tato připojení jsou nastavena podle popisu v příručce *IBM i Communication Configuration Reference*.

  V prostředí TCP je každé distribuované službě přidělena jedinečná adresa TCP, kterou mohou vzdálené počítače použít pro přístup ke službě. Adresa TCP se skládá z názvu/čísla hostitele a čísla portu. Všichni správci front používají takové číslo pro vzájemnou komunikaci prostřednictvím protokolu TCP.
- “Příjem na TCP” na stránce 278

Tento způsob komunikace vyžaduje definici IBM i logické jednotky SNA typu 6.2 (LU 6.2), která poskytuje fyzické propojení mezi systémem IBM i obsluhujícími lokálního správce front a systémem obsluhujícími vzdáleného správce front. Podrobnosti o konfiguraci komunikací v produktu IBM inaleznete v příručce *IBM i Communication Configuration Reference* .

V případě potřeby musí být spouštěcí mechanismus rovněž připraven s definováním nezbytných procesů a front.

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Související úlohy

“Monitorování a řízení kanálů na systému IBM i” na stránce 263
Pomocí panelů a příkazů DQM můžete vytvářet, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení s kompatibilními vzdálenými správci front.

Související odkazy

Příklad konfigurace- IBM MQ for IBM i
Příklad plánování kanálu zpráv pro IBM MQ for IBM i
Úlohy interkomunikace na systému IBM i
Stavy kanálů na systému IBM i

IBM i *Definování připojení TCP na systému IBM i*

Můžete definovat připojení TCP v rámci definice kanálu pomocí pole Název připojení.

Definice kanálu obsahuje pole CONNECTION NAME, které obsahuje buď síťovou adresu TCP cíle, nebo název hostitele (například ABCHOST). Síťová adresa TCP může být v tečkovém desítkovém formátu IPv4 (například 127.0.0.1) nebo IPv6 hexadecimálním formátu (například 2001:DB8:0:0:0:0:0:0). Je-li CONNECTION NAME název hostitele nebo server názvů, tabulka hostitelů IBM i se používá k převodu názvu hostitele na adresu hostitele TCP.

Pro úplnou adresu TCP je vyžadováno číslo portu. Není-li toto číslo zadáno, použije se výchozí číslo portu 1414. Na zahajovacím konci připojení (typ odesílatele, žadatele a kanálu serveru) je možné zadat volitelné číslo portu pro připojení, například:

```
Connection name 127.0.0.1 (1555)
```

V tomto případě se inicializační ukončení pokusí připojit k přijímajícímu programu na portu 1555.

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Použití volby nevyřízených požadavků modulu listener TCP

V protokolu TCP se s připojeními zachází jako s neúplnými, pokud mezi serverem a klientem nedojde k třícestnému navázání komunikace. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nevyřízené požadavky čekající na port TCP, aby mohl modul listener přijmout požadavek.

Další informace viz “Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému IBM MQ for Multiplatforms” na stránce 260 a specifická hodnota pro IBM i.

Související pojmy

“Příjem na TCP” na stránce 278

Programy přijímacího kanálu jsou spouštěny v reakci na spouštěcí požadavek odesílajícího kanálu. Chcete-li odpovědět na požadavek spuštění, musí být spuštěn program modulu listener, aby zjistil příchozí síťové požadavky a spustil přidružený kanál. Tento program listener spustíte příkazem STRMQMLSR.

IBM i *Příjem na TCP*

Programy přijímacího kanálu jsou spouštěny v reakci na spouštěcí požadavek odesílajícího kanálu. Chcete-li odpovědět na požadavek spuštění, musí být spuštěn program modulu listener, aby zjistil příchozí síťové požadavky a spustil přidružený kanál. Tento program listener spustíte příkazem STRMQMLSR.

Pro každého správce front můžete spustit více než jeden modul listener. Standardně příkaz STRMQMLSR používá port 1414, ale tuto hodnotu můžete přepsat. Chcete-li potlačit výchozí nastavení, přidejte následující příkazy do souboru qm.ini vybraného správce front. V tomto příkladu je modul listener vyžadován pro použití portu 2500:

```
TCP:
Port=2500
```

Soubor qm.ini se nachází v tomto adresáři IFS: /QIBM/UserData/mqm/qmgrs/ *název správce front*.

Tato nová hodnota je jen pro čtení, když je spuštěn modul listener TCP. Máte-li již spuštěný modul listener, tuto změnu tento program neuvidí. Chcete-li použít novou hodnotu, zastavte modul listener a zadejte příkaz STRMQMLSR znovu. Nyní, kdykoli použijete příkaz STRMQMLSR, modul listener standardně použije nový port.

Případně můžete v příkazu STRMQMLSR zadat jiné číslo portu. Příklad:

```
STRMQMLSR MQMNAME( queue manager name ) PORT(2500)
```

Tato změna nastaví modul listener jako výchozí pro nový port po dobu trvání úlohy modulu listener.

Použití volby TCP SO_KEEPALIVE

Chcete-li použít volbu SO_KEEPALIVE (další informace viz "Kontrola, zda je druhý konec kanálu stále k dispozici" na stránce 225) Do konfiguračního souboru správce front (qm.ini v adresáři IFS /QIBM/UserData/mqm/qmgrs/ *název správce front*) musíte přidat následující položku:

```
TCP:
KeepAlive=yes
```

Poté musíte zadat následující příkaz:

```
CFGTCP
```

Vyberte volbu 3 (Změna atributů TCP). Nyní můžete zadat časový interval v minutách. Můžete uvést hodnotu v rozsahu 1 až 40320 minut; předvolba je 120.

Použití volby nevyřízených požadavků modulu listener TCP

Při příjmu prostřednictvím protokolu TCP je nastaven maximální počet nevyřízených požadavků na připojení. Tento počet lze považovat za *nevyřízené* požadavky čekající na port TCP, aby modul listener přijal požadavek.

Výchozí hodnota seznamu požadavků modulu listener na systému IBM i je 255. Pokud nevyřízené požadavky dosáhnou této hodnoty, připojení TCP je odmítnuto a kanál není schopen se spustit.

V případě kanálů MCA to má za následek, že kanál přejde do stavu OPAKOVAT a později se znovu pokusí o připojení.

V případě připojení klienta klient obdrží od MQCONN kód příčiny MQRC_Q_MGR_NOT_AVAILABLE a může připojení zopakovat později.

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

```
ListenerBacklog = n
```

Toto potlačí výchozí maximální počet neprovedených požadavků (255) pro modul listener TCP.

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí hodnota. V případě potřeby lze tuto hodnotu použít, aby se zabránilo dosažení limitu připojení.

IBM i *Definování připojení LU 6.2 na systému IBM i*

Definujte podrobnosti komunikace LU 6.2 pomocí jména režimu, jména TP a jména připojení plně kvalifikovaného připojení LU 6.2 .

Iniciovaný konec linky musí mít definici položky směrování, která bude doplňovat tento objekt CSI. Další informace o správě pracovních požadavků ze vzdálených systémů LU 6.2 jsou k dispozici v příručce *IBM i Programming: Work Management Guide*.

Informace naleznete v příručce *Multiplatform APPC Configuration Guide* a v následující tabulce.

Tabulka 25. Nastavení v lokálním systému IBM i pro vzdálenou platformu správce front

Vzdálená platforma	**TPNAME**
z/OS nebo MVS	Stejné jako v odpovídajících vedlejších informacích o vzdáleném správci front.
IBM i	Stejná hodnota jako porovnávací hodnota v záznamu směrování v systému IBM i .
Systémy AIX and Linux	Vyvolatelný transakční program definovaný v konfiguraci vzdálené LU 6.2 .
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo v vyvolatelném transakčním programu, který byl definován pomocí TpSetup na systému Windows.

Máte-li ve stejném počítači více než jednoho správce front, zkontrolujte, zda jsou názvy TPname v definicích kanálu jedinečné.

Související pojmy

“Zahajovací konec (odesílatel)” na stránce 279
Pomocí příkazu CRTMQMCHL definujte kanál typu přenosu *LU62.

“Zahájený konec (přijímač)” na stránce 282
Pomocí příkazu CRTMQMCHL definujte přijímající konec propojení kanálu zpráv s typem přenosu *LU62.

IBM i *Zahajovací konec (odesílatel)*

Pomocí příkazu CRTMQMCHL definujte kanál typu přenosu *LU62.

Použití objektu CSI je v produktu IBM MQ for IBM i V5.3 nebo novějším volitelné.

Počáteční koncový panel je znázorněn na obrázku LU 6.2 panel nastavení komunikace-inicializační konec. Chcete-li získat úplný panel, jak je zobrazeno, stiskněte klávesu F10 z prvního panelu.

```
Create Comm Side Information (CRTCSI)

Type choices, press Enter.

Side information . . . . . > WINSDOA1   Name
Library . . . . . >  QSYS    Name, *CURLIB
Remote location . . . . . > WINSDOA1   Name
Transaction program . . . . . > MQSERIES

Text 'description' . . . . . .  *BLANK


Additional Parameters

Device . . . . . .  *LOC     Name, *LOC
Local location . . . . . .  *LOC     Name, *LOC, *NETATR
Mode . . . . . .  JSTMOD92   Name, *NETATR
Remote network identifier . . .  *LOC     Name, *LOC, *NETATR, *NONE
Authority . . . . . .  *LIBCRTAUT  Name, *LIBCRTAUT, *CHANGE...

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 34. Panel nastavení komunikace LU 6.2 -zahájení ukončení

Vyplňte pole konce zahájení následujícím způsobem:

Informace o straně
Zadejte pro tuto definici název používaný k uložení objektu informací o straně, který má být vytvořen, například WINSDOA1.

Poznámka: V případě LU 6.2je propojení mezi definicí kanálu zpráv a komunikačním připojením pole **Jméno připojení** definice kanálu zpráv na odesílajícím konci. Toto pole obsahuje název objektu CSI.

Knihovna
Název knihovny, kde je tato definice uložena.

Objekt CSI musí být k dispozici v knihovně přístupné pro program obsluhující kanál zpráv, například QSYS, QMQM a QGPL.

Pokud je název nesprávný, chybí nebo nebyl nalezen, dojde při spuštění kanálu k chybě.

Vzdálené umístění
Uvádí název vzdáleného systému, se kterým váš program komunikuje.

Stručně řečeno, tento požadovaný parametr obsahuje název logické jednotky partnera na vzdáleném systému, jak je definováno v popisu zařízení, který se používá pro komunikační spojení mezi těmito dvěma systémy.

Název **Vzdálené umístění** lze nalézt zadáním příkazu DSPNETA na vzdáleném systému a prohlédnutí předvoleného názvu lokálního systému.

Transakční program
Uvádí název (až 64 znaků) transakčního programu na vzdáleném systému, který se má spustit. Může se jednat o název procesu transakce, název programu, název kanálu nebo znakový řetězec, který odpovídá **porovnávací hodnotě** v položce směrování.

Tento parametr je požadovaný.

Poznámka: Chcete-li zadat názvy programů servisních transakcí SNA, zadejte hexadecimální reprezentaci názvu programu servisních transakcí. Chcete-li například zadat název programu servisní transakce s hexadecimální reprezentací 21F0F0F1, zadejte hodnotu X'21F0F0F1'.

Další informace o názvech servisních transakčních programů SNA naleznete v příručce *SNA Transaction Programmer's Reference* pro LU typu 6.2.

Je-li přijímacím koncem jiný systém IBM i , použije se název **Transakčního programu** pro shodu objektu CSI na odesílajícím konci se záznamem směrování na přijímajícím konci. Tento název musí

být jedinečný pro každého správce front v cílovém systému IBM i . Viz parametr **Program pro volání** v části Iniciovaný konec (přijímač). Viz také parametr **Porovnání dat: porovnávací hodnota** na panelu Přidat položku směrování.

Textový popis
Popis (až 50 znaků), který vám připomene zamýšlené použití tohoto připojení.

Zařízení
Uvádí název popisu zařízení použitého pro vzdálený systém. Možné hodnoty jsou:

***LOC**
Zařízení je určeno systémem.

Název zařízení
Uveďte název zařízení, které je přidruženo ke vzdálenému umístění.

Lokální umístění
Určuje název lokálního umístění. Možné hodnoty jsou:

***LOC**
Název lokálního umístění je určen systémem.

***NETATR**
Použije se hodnota LCLLOCNAME uvedená v systémových atributech sítě.

Název-lokálního-umístění
Zadejte název svého umístění. Uveďte lokální umístění, pokud chcete označit specifický název umístění pro vzdálené umístění. Název umístění lze nalézt pomocí příkazu DSPNETA.

Režim
Určuje režim používaný k řízení relace. Tento název je stejný jako název CPI (Common Programming Interface)-Communications Mode_Name. Možné hodnoty jsou:

***NETATR**
Použije se režim v atributech sítě.

BLANK
Použije se osm prázdných znaků.

Název režimu
Zadejte název režimu pro vzdálené umístění.

Poznámka: Vzhledem k tomu, že režim určuje prioritu přenosu komunikační relace, může být užitečné definovat různé režimy v závislosti na prioritě odesílaných zpráv, například MQMODE_HI, MQMODE_MED a MQMODE_LOW. (Můžete mít více než jeden CSI ukazující na stejné umístění.)

Identifikátor vzdálené sítě
Uvádí identifikátor vzdálené sítě použitý se vzdáleným umístěním. Možné hodnoty jsou:

***LOC**
Použije se ID vzdálené sítě pro vzdálené umístění.

***NETATR**
Použije se identifikátor vzdálené sítě uvedený v atributech sítě.

***NONE**
Vzdálená síť nemá žádný název.

ID-vzdálené-sítě
Zadejte ID vzdálené sítě. Použijte příkaz DSPNETA na vzdáleném systému, abyste nalezli název tohoto ID sítě. Jedná se o 'ID lokální sítě' ve vzdáleném umístění.

Oprávnění
Uvádí oprávnění, které poskytujete uživatelům, kteří nemají specifické oprávnění k objektu, kteří nejsou na seznamu oprávnění, a s profilem skupiny, který nemá specifické oprávnění k objektu. Možné hodnoty jsou:

***LIBCRTAUT**
Obecné oprávnění pro objekt je převzato z parametru CRTAUT uvedené knihovny. Tato hodnota je určena v čase vytvoření. Pokud se hodnota CRTAUT pro knihovnu změní po vytvoření objektu, nová hodnota neovlivní existující objekty.

***CHANGE (změna)**
Oprávnění ke změně umožňuje uživateli provádět základní funkce na objektu, avšak uživatel nemůže objekt změnit. Oprávnění ke změně poskytuje provozní oprávnění k objektu a všechna oprávnění k datům.

***ALL**
Uživatel může provádět všechny operace kromě operací omezených na vlastníka nebo řízených oprávněním pro správu seznamu oprávnění. Uživatel může řídit existenci objektu a určit zabezpečení objektu, změnit objekt a provést základní funkce na objektu. Uživatel může změnit vlastnictví objektu.

***USE**
Oprávnění k použití poskytuje provozní oprávnění k objektu a oprávnění ke čtení.

***EXCLUDE**
Oprávnění k vyloučení brání uživateli v přístupu k objektu.

Seznam oprávnění
Uveďte název seznamu oprávnění s oprávněním, který se používá pro informace o straně.

IBM i *Zahájený konec (přijímač)*

Pomocí příkazu CRTMQMCHL definujte přijímající konec propojení kanálu zpráv s typem přenosu *LU62.

Ponechte pole CONNECTION NAME prázdné a ujistěte se, že odpovídající podrobnosti odpovídají odesílajícímu konci kanálu. Podrobnosti naleznete v tématu Vytvoření kanálu.

Chcete-li povolit inicializační ukončení pro spuštění přijímacího kanálu, přidejte záznam směrování do subsystému na zahájeném konci. Subsystém musí být ten, který přiděluje zařízení APPC použité v relacích LU 6.2 . Proto musí mít platný komunikační záznam pro toto zařízení. Záznam směrování volá program, který spouští přijímací konec kanálu zpráv.

Pomocí příkazů IBM i (například ADDRTGE) definujte konec spoje, který je iniciován komunikační relací.

Iniciovaný koncový panel je zobrazen v panelu nastavení komunikace LU 6.2 -přidání záznamu směrování.

```
Add Routing Entry (ADDRTGE)

Type choices, press Enter.

Subsystem description . . . . .  QCMN     Name
Library . . . . . .   *LIBL    Name, *LIBL, *CURLIB
Routing entry sequence number .  1       1-9999
Comparison data:
Compare value . . . . . .  MQSERIES

Starting position . . . . . .  37      1-80
Program to call . . . . . .  AMQCRC6B   Name, *RTGDTA
Library . . . . . .  QMAS400    Name, *LIBL, *CURLIB
Class . . . . . .  *SBSD     Name, *SBSD
Library . . . . . .  *LIBL     Name, *LIBL, *CURLIB
Maximum active routing steps . .  *NOMAX    0-1000, *NOMAX
Storage pool identifier . . . .  1       1-10



Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 35. Ukončení zahájeného panelu nastavení komunikace LU 6.2

Popis subsystému
Název subsystému, kde se tato definice nachází. Použijte příkaz IBM i WRKSBSD k zobrazení a aktualizaci odpovídajícího popisu subsystému pro směrovací záznam.

Pořadové číslo záznamu směrování
Jedinečné číslo v subsystému pro identifikaci této definice komunikace. Můžete použít hodnoty v rozsahu 1-9999.

Porovnávací data: Porovnat hodnotu
Textový řetězec, který se má porovnat s řetězcem přijatým při spuštění relace parametrem **Transakční program** , jak ukazuje Obrázek 1. Znakový řetězec je odvozen z pole Transaction program CSI odesilatele.

Porovnávací data: počáteční pozice
Pozice znaku v řetězci, kde má začít porovnání.

Poznámka: Pole počáteční pozice je znaková pozice v řetězci pro porovnání a tato pozice je vždy 37.

Program pro volání
Název programu, který spouští program příchozí zprávy, který má být volán pro spuštění relace.

Pro výchozího správce front je volán program AMQCRC6A. Tento program je dodáván s produktem IBM MQ for IBM i a nastavuje prostředí a pak volá AMQCRS6A.

Pro další správce front:

- Každý správce front má specifický vyvolatelný program LU 6.2 umístěný ve své knihovně. Tento program se nazývá AMQCRC6B a je automaticky generován při vytvoření správce front.
- Každý správce front vyžaduje přidání specifické položky směrování s jedinečnými daty směrování. Tato data směrování se musí shodovat s názvem **Transakčního programu** dodaným požadujícím systémem (viz Initiating end (Sender)).

Příklad je uveden na panelu nastavení komunikace LU 6.2 -zobrazení záznamů směrování:

```
Display Routing Entries
System:  MY400
Subsystem description:  QCMN      Status:  ACTIVE

Type options, press Enter.
5=Display details

Start
Opt  Seq Nbr  Program    Library    Compare Value   Pos
10   *RTGDTA           'QZSCSRVR'     37
20   *RTGDTA           'QZRCSRVR'     37
30   *RTGDTA           'QZHQTRG'     37
50   *RTGDTA           'QVPPRINT'     37
60   *RTGDTA           'QNPSERVR'     37
70   *RTGDTA           'QNMAPINGD'    37
80   QNMAREXECD  QSYS     'AREXECD'     37
90   AMQCRC6A   QMQMBW    'MQSERIES'     37
100   *RTGDTA           'QTFDWNLD'     37
150   *RTGDTA           'QMFRCVR'     37



F3=Exit  F9=Display all detailed descriptions  F12=Cancel
```

Obrázek 36. Ukončení zahájeného panelu nastavení komunikace LU 6.2

V panelu LU 6.2 nastavení komunikace-zobrazení položek směrovánípředstavuje pořadové číslo 90 výchozího správce front a poskytuje kompatibilitu s konfiguracemi z předchozích verzí (tj. V3R2, V3R6, V3R7a V4R2) produktu IBM MQ for IBM i. Tato vydání povolují pouze jednoho správce front. Pořadová čísla 92 a 94 představují dva další správce front s názvem ALPHA a BETA, kteří jsou vytvořeni s knihovnami QMALPHA a QMBETA.

Poznámka: Pro každého správce front můžete mít více než jednu položku směrování s použitím různých dat směrování. Tyto záznamy poskytují volbu různých priorit úloh v závislosti na použitých třídách.

Třída
Název a knihovna třídy použité pro kroky spuštěné prostřednictvím tohoto záznamu směrování. Třída definuje atributy spuštěného prostředí směrovacího kroku a určuje prioritu úlohy. Musí být uveden odpovídající záznam třídy. Použijte například příkaz WRKCLS k zobrazení existujících tříd nebo k vytvoření třídy. Další informace o správě pracovních požadavků ze vzdálených systémů LU 6.2 jsou k dispozici v příručce *IBM i Programming: Work Management Guide*.

Poznámka ke správě činnosti systému

Úloha AMQCRS6A nemůže využít běžných funkcí správy činnosti systému IBM i , které jsou dokumentovány v části Správa činnosti systému , protože není spuštěna stejným způsobem jako ostatní úlohy IBM MQ . Chcete-li změnit běhové vlastnosti úloh příjemce LU62 , můžete provést jednu z následujících změn:

- Změňte popis třídy, který je uveden v záznamu směrování pro úlohu AMQCRS6A .
- Změna popisu úlohy v komunikačním záznamu

Další informace o konfiguraci komunikačních úloh naleznete v příručce *IBM i Programming: Work Management Guide* .

Konfigurace klastru správců front

Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

Než začnete

Úvod do koncepcí klastrování viz Klastry.

Při navrhování klastru správců front je třeba provést určitá rozhodnutí. Viz Vzorové klastry a Návrh klastrů.

Související úlohy
“Přesunutí definice tématu klastru do jiného správce front” na stránce 428
V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Související odkazy
Odstranit téma

Definování komponent klastru

Klastry se skládají ze správců front, kanálů klastru a front klastru. Můžete definovat fronty klastru a upravit některé aspekty výchozích objektů klastru. Můžete získat informace o konfiguraci a stavu automaticky definovaných kanálů a o vztahu mezi jednotlivými odesílacími kanály klastru a přenosovými frontami.

Informace o definování jednotlivých komponent klastru naleznete v následujících dílčích tématech:

Související pojmy
Komponenty klastru
Kanály klastru
Související úlohy
Definování témat klastru
“Nastavení nového klastru” na stránce 297

Postupujte podle těchto pokynů, abyste nastavili ukázkový klastr. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosovými frontami. Otestujte práci klastru odesláním zprávy z jednoho správce front do druhého.

“Přidání správce front do klastru” na stránce 308
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů.
Zprávy do front klastru a témata se přenášejí pomocí jedné přenosové fronty klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Definování front klastru

Fronta klastru je fronta, jejímž hostitelem je správce front klastru, a která je dostupná ostatním správcům front v klastru.Definujte frontu klastru jako lokální frontu ve správci front klastru, kde je fronta hostována. Zadejte název klastru, do kterého fronta patří.

Následující příklad ukazuje příkaz **runmqsc** pro 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.

z/OS Fronta klastru může být fronta, kterou sdílí členové skupiny sdílení front v produktu IBM MQ for z/OS.

Vazba

Můžete vytvořit klastr, ve kterém je více než jeden správce front hostitelem instance stejné fronty klastru. Ujistěte se, že všechny zprávy v posloupnosti jsou odeslány do stejné instance fronty. Posloupnost zpráv můžete svázat s konkrétní frontou pomocí volby MQOO_BIND_ON_OPEN ve volání MQOPEN .

Přenosové fronty klastru

Správce front může ukládat zprávy pro ostatní správce front z klastru do více přenosových front. Správce front můžete nakonfigurovat tak, aby ukládal zprávy do více přenosových front klastru, dvěma různými způsoby. Nastavíte-li atribut správce front **DEFCLXQ** na hodnotu CHANNEL, bude pro každý odesílací kanál klastru v produktu SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE automaticky vytvořena odlišná přenosová fronta klastru. Pokud nastavíte volbu přenosové fronty CLCHNAME tak, aby se shodovala s jedním nebo více odesílacími kanály klastru, bude správce front moci ukládat zprávy pro odpovídající kanály do těchto přenosových front.

Upozornění: Používáte-li vyhrazenou hodnotu SYSTEM.CLUSTER.TRANSMIT.QUEUES se správcem front, který byl upgradován z verze produktu starší než IBM WebSphere MQ 7.5, ujistěte se, že má SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE volbu SHARE/NOSHARE nastavenou na hodnotu **SHARE**.

Zpráva pro frontu klastru v jiném správci front je před odesláním umístěna do přenosové fronty klastru. Odesílací kanál klastru přenáší zprávy z přenosové fronty klastru do přijímacích kanálů klastru v jiných správcích front. Při výchozím nastavení obsahuje 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 v této přenosové frontě klastru jinému správci front ve stejném klastru.

Definice pro jednotlivou frontu SYSTEM.CLUSTER.TRANSMIT.QUEUE je standardně vytvořena v každém správci front kromě z/OS. z/OS V systému z/OSlze definici definovat s dodanou ukázkou **CSQ4INSX**.

Správce front lze konfigurovat pro přenos zpráv do jiných klastrovaných správců front pomocí více přenosových front. Další přenosové fronty klastru můžete definovat ručně nebo nechat správce front vytvořit fronty automaticky.

Chcete-li vytvořit fronty automaticky správcem front, změňte atribut správce front DEFCLXQ z SCTQ na CHANNEL. Výsledkem je, že správce front vytvoří individuální přenosovou frontu klastru pro každý vytvořený odesílací kanál klastru. Přenosové fronty jsou vytvořeny 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 každá trvalá přenosová fronta dynamického klastru, je nastaven v atributu lokální přenosové fronty CLCHNAME. Zprávy pro vzdálené klastrované správce front jsou umístěny do trvalé přenosové fronty dynamického klastru pro přidružený odesílací kanál klastru, nikoli do systému SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Chcete-li vytvořit přenosové fronty klastru ručně, vytvořte lokální frontu s atributem USAGE nastaveným na hodnotu XMITQa atribut CLCHNAME nastavte na generický název kanálu, který se interpretuje na jeden nebo více odesílacích kanálů klastru; viz ClusterChannel. Pokud vytváříte přenosové fronty klastru ručně, máte možnost přidružit přenosovou frontu k jednomu odesílacímu kanálu klastru nebo k více odesílacím kanálům klastru. Atribut CLCHNAME je generický název, což znamená, že do názvu můžete umístit více zástupných znaků "*".

S výjimkou počátečních odesílacích kanálů klastru, které vytvoříte ručně pro připojení správce front k úplnému úložišti, jsou odesílací kanály klastru vytvářeny automaticky. Jsou vytvořeny automaticky, když existuje zpráva, která se má přenést do správce front klastru. Jsou vytvořeny se stejným názvem jako název přijímacího kanálu klastru, který přijímá zprávy klastru pro daný klastr v cílovém správci front.

Pokud dodržujete konvenci pojmenování pro přijímací kanály klastru, je možné definovat generickou hodnotu pro CLCHNAME , která filtruje různé druhy zpráv klastru do různých přenosových front. Pokud například dodržujete konvenci pojmenování pro přijímací kanály klastru *ClusterName*. *QmgrName*, pak generický název *ClusterName*.* filtruje zprávy pro různé klastry do různých přenosových front. Přenosové fronty musíte definovat ručně a nastavit CLCHNAME v každé přenosové frontě na *ClusterName*.*.

Změny přidružení přenosových front klastru k odesílacím kanálům klastru se neprojeví okamžitě. Aktuálně přidružená přenosová fronta, kterou obsluhuje odesílací kanál klastru, může obsahovat zprávy, které jsou v procesu přenosu odesílacím kanálem klastru. Pouze v případě, že odesílací kanál klastru nezpracovává žádné zprávy v aktuálně přidružené přenosové frontě, může správce front změnit přidružení odesílacího kanálu klastru na jinou přenosovou frontu. K tomu může dojít buď v případě, že v přenosové frontě nezůstanou žádné zprávy ke zpracování odesílacím kanálem klastru, nebo když je zpracování zpráv pozastaveno a odesílací kanál klastru nemá žádné "probíhající" zprávy. Pokud k tomu dojde, všechny nezpracované zprávy pro odesílací kanál klastru se přenesou do nově přidružené přenosové fronty a změní se přidružení odesílacího kanálu klastru.

Můžete vytvořit definici vzdálené fronty, která se interpretuje jako přenosová fronta klastru. V definici je správce front QMX ve stejném klastru jako lokální správce front a neexistuje žádná přenosová fronta QMX.

```
DEFINE QREMOTE(A) RNAME(B) RQMNAME(QMX)
```

Během rozpoznávání názvů front má přenosová fronta klastru přednost před výchozí přenosovou frontou. Zpráva vložená 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 přenosovou frontu musíte definovat do druhého správce front stejným způsobem jako v prostředí distribuovaných front.

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. Přidá do zprávy informace o směrování a vloží je do přenosové fronty klastru. Produkt IBM MQ automaticky vytvoří definici ekvivalentní definici vzdálené fronty, aby mohla být zpráva odeslána.

Automaticky vytvořenou definici vzdálené fronty nelze změnit ani odstranit. Pomocí příkazu DISPLAY QUEUE **runmqsc** s atributem CLUSINFO však můžete zobrazit všechny lokální fronty ve správci front i všechny fronty klastru, včetně front klastru ve vzdálených správcích front. Příklad:

```
DISPLAY QUEUE(*) CLUSINFO
```

Související pojmy

Fronty klastru

Jak vybrat typ přenosové fronty klastru, který se má použít

Související odkazy

ClusterChannelNázev (MQCHAR20)

Práce s automaticky definovanými odesílacími kanály klastru

Po zavedení správce front do klastru provedením jeho počátečních definic CLUSSDR a CLUSRCVR produkt IBM MQ automaticky vytvoří další definice odesílacího kanálu klastru, je-li třeba přesunout zprávy do jiného správce front v klastru. Můžete zobrazit informace o automaticky definovaných odesílacích kanálech klastru, ale nemůžete je upravit. Chcete-li upravit jejich chování, můžete použít uživatelskou proceduru automatické definice kanálu.

Než začnete

Úvod k automaticky definovaným kanálům naleznete v tématu Automaticky definované odesílací kanály klastru.

Informace o této úloze

Automaticky definované odesílací kanály klastru jsou vytvářeny klastrem podle potřeby a zůstávají aktivní, dokud nejsou ukončeny pomocí pravidel normálního intervalu odpojení.

Odesílací kanály klastru (CLUSSDR) mohou být automaticky definovány jak pro přesun zpráv aplikace, tak pro interní zprávy administrace klastru. Například v klastru publikování/odběru (v němž bylo definováno klastrované téma) lze definovat kanály mezi dílčími úložišti, aby bylo možné povolit výměnu stavu 'proxy odběr'. Není-li vyžadováno (neaktivní) po delší dobu, jsou automaticky definované rutiny CLUSSDR odebrány z mezipaměti částečného úložiště s informacemi o klastru a již nejsou v tomto správci front viditelné.

Multi V systému Multiplatformsnení OAM (správce oprávnění k objektu) informován o existenci automaticky definovaných odesílacích kanálů klastru. Zadáte-li příkazy **start**, **stop**, **ping**, **reset**nebo **resolve** v automaticky definovaném odesílacím kanálu klastru, OAM zkontroluje, zda máte oprávnění provádět stejnou akci na odpovídajícím přijímacím kanálu klastru.

z/OS V systému z/OSmůžete automaticky definovaný odesílací kanál klastru zabezpečit stejným způsobem jako kterýkoli jiný kanál.

Procedura

- Zobrazí informace o automaticky definovaných kanálech pro daného správce front klastru.

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

```
DISPLAY CLUSQMGR(qMgrName)
```

- Zobrazí stav automaticky definovaného kanálu pro daný CLUSRCVR.

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

  ```
  DISPLAY CHSTATUS(channelname)
  ```

- Pomocí uživatelské procedury automatické definice kanálu upravte chování automaticky definovaného kanálu.

  Uživatelskou proceduru automatické definice kanálu IBM MQ můžete použít, chcete-li napsat uživatelský program, abyste přizpůsobili kanál odesilatele klastru nebo kanál příjemce klastru. Můžete například použít uživatelskou proceduru automatické definice kanálu v klastrovaném prostředí a provést některou z následujících úprav:

  - Přizpůsobte definice komunikací, tj. názvy SNA LU6.2 .
  - Přidejte nebo odeberte další uživatelské procedury, například uživatelské procedury zabezpečení.
  - Změňte názvy uživatelských procedur kanálu.

    Název uživatelské procedury kanálu CLUSSDR je automaticky generován z definice kanálu CLUSRCVR , a proto nemusí odpovídat vašim potřebám-zejména pokud jsou oba konce kanálu na různých platformách.

    Formát názvů uživatelských procedur se na různých platformách liší. Příklad:

    - z/OS Na platformě z/OS je formát parametru SCYEXIT (*název uživatelské procedury zabezpečení*) SCYEXIT('SECEXIT') .
    - Windows Na platformách Windows je formát parametru SCYEXIT (*název uživatelské procedury zabezpečení*) SCYEXIT(' *drive*:*path**library* (secexit)') .

    Poznámka: z/OS Pokud neexistuje žádná uživatelská procedura automatické definice kanálu, správce front z/OS odvozuje název uživatelské procedury kanálu CLUSSDR z definice kanálu CLUSRCVR na druhém konci kanálu. Chcete-li odvodit název uživatelské procedury z/OS z jiného názvu nežz/OS , použije se následující algoritmus:

    - Názvy ukončení v systému Multiplatforms jsou v obecném formátu *cesta*/*knihovna* (*funkce*).
    - Je-li přítomna *funkce* , použije se až osm znaků.
    - Jinak se použije až osm znaků *knihovny* .

    Příklad:

    - /var/mqm/exits/myExit.so(MsgExit) se převede na MSGEXIT
    - /var/mqm/exits/myExit se převede na MYEXIT
    - /var/mqm/exits/myExit.so(ExitLongName) se převede na EXITLONG

  - Pokud klastr potřebuje použít produkt **PROPCTL** k odebrání záhlaví aplikace, jako např. RFH2 , ze zpráv ze správce front IBM MQ do správce front v dřívější verzi produktu, musíte napsat uživatelskou proceduru automatické definice kanálu, která nastaví **PROPCTL** na hodnotu NONE.

- K řízení aspektů adresování použijte atribut kanálu LOCLADDR .
  - Chcete-li povolit, aby odchozí kanál (TCP) používal konkrétní adresu IP, port nebo rozsah portů, použijte atribut kanálu LOCLADDR. To je užitečné v případě, že máte více než jednu síťovou kartu a chcete, aby kanál používal pro odchozí komunikaci specifickou síťovou kartu.

- Chcete-li zadat virtuální adresu IP na kanálech CLUSSDR , použijte adresu IP z LOCLADDR na ručně definované CLUSSDR. Chcete-li určit rozsah portů, použijte rozsah portů z CLUSRCVR.
- Pokud klastr potřebuje použít příkaz LOCLADDR k získání odchozích komunikačních kanálů pro vytvoření vazby na specifickou adresu IP, můžete napsat uživatelskou proceduru automatické definice kanálu, která vynutí hodnotu LOCLADDR do některého z automaticky definovaných kanálů CLUSSDR . Musíte jej také zadat v ručně definovaném kanálu CLUSSDR .
- Zadejte číslo portu nebo rozsah portů do pole LOCLADDR kanálu CLUSRCVR , chcete-li, aby všichni správci front v klastru používali specifický port nebo rozsah portů pro všechny odchozí komunikace.

Poznámka: Neukládejte adresu IP do pole LOCLADDR kanálu CLUSRCVR , pokud nejsou všichni správci front na stejném serveru. Adresa IP LOCLADDR je šířena do automaticky definovaných kanálů CLUSSDR všech správců front, kteří se připojují pomocí kanálu CLUSRCVR .

Multi V systému Multiplatformsmůžete nastavit výchozí hodnotu lokální adresy, která se použije pro všechny odesílací kanály, které nemají definovanou lokální adresu. Výchozí hodnota je definována nastavením proměnné prostředí MQ_LCLADDR před spuštěním správce front. Formát hodnoty odpovídá formátu atributu MQSC LOCLADDR.

Související odkazy

Lokální adresa (LOCLADDR)

Práce s výchozími objekty klastru

Spuštěním příkazů MQSC nebo PCF můžete změnit výchozí definice kanálů stejným způsobem jako libovolnou jinou definici kanálu. Neměňte výchozí definice front, s výjimkou SYSTEM.CLUSTER.HISTORY.QUEUE.

Úplný seznam těchto objektů naleznete v tématu Výchozí objekty klastru. Následující seznam obsahuje pouze ty objekty, které můžete změnit.

SYSTEM.CLUSTER.HISTORY.QUEUE

Každý správce front v klastru má lokální frontu s názvem SYSTEM.CLUSTER.HISTORY.QUEUE. SYSTEM.CLUSTER.HISTORY.QUEUE se používá k uložení historie informací o stavu klastru pro servisní účely.

Ve výchozím nastavení objektu je parametr SYSTEM.CLUSTER.HISTORY.QUEUE nastaven na hodnotu PUT (ENABLED). Chcete-li potlačit kolekci historie, změňte nastavení na PUT (DISABLED).

SYSTEM.CLUSTER.TRANSMIT.QUEUE

Každý správce front má definici pro lokální frontu s názvem SYSTEM.CLUSTER.TRANSMIT.QUEUE. SYSTEM.CLUSTER.TRANSMIT.QUEUE je výchozí přenosová fronta pro všechny zprávy pro všechny fronty a správce front v rámci klastrů. Výchozí přenosovou frontu pro každý odesílací kanál klastru můžete změnit na hodnotu SYSTEM.CLUSTER.TRANSMIT.*ChannelName*změnou atributu správce front DEFXMITQ z/OS , s výjimkou systému z/OS . Nelze odstranit SYSTEM.CLUSTER.TRANSMIT.QUEUE. Používá se také k definování kontrol autorizace, zda je použita výchozí přenosová fronta SYSTEM.CLUSTER.TRANSMIT.QUEUE nebo SYSTEM.CLUSTER.TRANSMIT.*ChannelName*.

Související pojmy

Výchozí objekty klastru

Práce s přenosovými frontami klastru a odesílacími kanály klastru

Zprávy mezi klastrovanými správci front jsou uloženy v přenosových frontách klastru a předávány odesílacími kanály klastru. V libovolném časovém okamžiku je odesílací kanál klastru přidružen k jedné přenosové frontě. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizované a transakční.

Spuštěním následujícího příkazu MQSC zobrazte přenosové fronty, ke kterým jsou odesílací kanály 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 ve stavu uloženého kanálu zastaveného odesílacího kanálu klastru se může změnit při opětovném spuštění kanálu. "Výběr výchozích přenosových front podle odesílacích kanálů klastru" na stránce 290 popisuje proces výběru výchozí přenosové fronty; "Výběr ručně definovaných přenosových front podle odesílacích kanálů klastru" na stránce 291 popisuje proces výběru ručně definované přenosové fronty.

Když se spustí některý odesílací kanál klastru, znovu zkontroluje jeho přidružení k přenosovým frontám. Pokud se změní konfigurace přenosových front nebo výchozí nastavení správce front, může dojít k opětovnému přidružení kanálu s jinou přenosovou frontou. Pokud se kanál v důsledku změny konfigurace restartuje s jinou přenosovou frontou, dojde k přenosu zpráv do nově přidružené přenosové fronty. "Jak proces přepnutí odesílacího kanálu klastru na jinou přenosovou frontu pracuje" na stránce 292 popisuje proces přenosu odesílacího kanálu klastru z jedné přenosové fronty do jiné.

Chování odesílacích kanálů klastru se liší od odesílacích kanálů a kanálů serveru. Zůstávají přidruženy ke stejné přenosové frontě, dokud není změněn atribut kanálu **XMITQ** . Pokud změníte atribut přenosové fronty v kanálu odesilatele nebo serveru a restartujete jej, zprávy se nepřenesou ze staré přenosové fronty do nové.

Další rozdíl mezi odesílacími kanály klastru a odesílacími kanály nebo kanály serveru spočívá v tom, že více odesílacích kanálů klastru může otevřít přenosovou frontu klastru, ale pouze jeden odesílací kanál nebo kanál serveru může otevřít normální přenosovou frontu. Můžete zvolit odesílací kanály klastru, které nesdílí přenosové fronty. Exkluzivita není vynucována; je to výsledek konfigurace. Cestu, kterou má zpráva v klastru, můžete konfigurovat tak, aby nesdílely žádné přenosové fronty nebo kanály se zprávami, které proudí mezi jinými aplikacemi. Viz Klastrování: Plánování konfigurace přenosových front klastru a "Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaných ze správce front brány" na stránce 341.

Výběr výchozích přenosových front podle odesílacích kanálů klastru

Přenosová fronta klastru je buď výchozí systémová fronta s názvem začínajícím na SYSTEM.CLUSTER.TRANSMIT, nebo ručně definovaná fronta. Odesílací kanál klastru je přidružen k přenosové frontě klastru jedním ze dvou způsobů: výchozím mechanismem přenosové fronty klastru nebo ruční konfigurací.

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

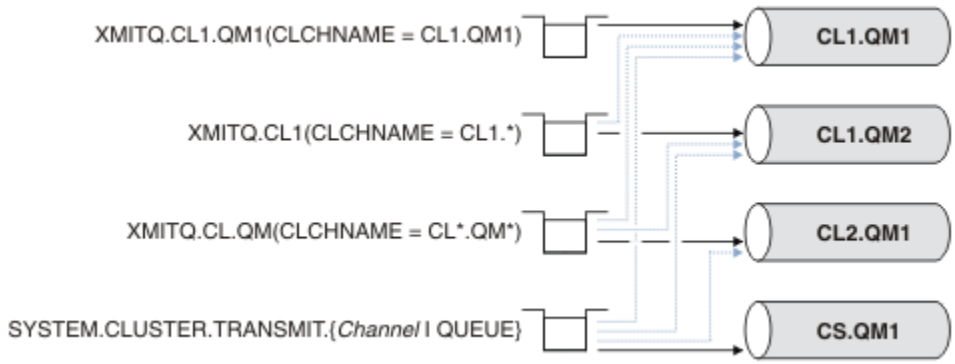
Je-li nastavena hodnota SCTQ , výchozí přenosová fronta klastru je SYSTEM.CLUSTER.TRANSMIT.QUEUE. Tuto frontu může otevřít každý odesílací kanál klastru. Odesílací kanály klastru, které otevírají frontu, jsou ty, které nejsou přidruženy k ručně definovaným přenosovým frontám klastru.

Je-li nastavena hodnota 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 přenosové frontě trvalého dynamického

klastru. Fronta je vytvořena správcem front, pokud vyžaduje samostatnou přenosovou frontu klastru pro cíl klastru obsluhovaný tímto kanálem odesilatele klastru, a neexistuje žádná fronta.

Některá místa určení klastru mohou být obsluhována odesílacími kanály klastru přidruženými k ručně definovaným přenosovým frontám a jiná výchozí frontou nebo frontami. V přidružení odesílacích kanálů klastru k přenosovým frontám mají ručně definované přenosové fronty vždy přednost před výchozími přenosovými frontami.

Přednost přenosových front klastru je znázorněna v tématu Obrázek 37 na stránce 291. Jediný odesílací kanál klastru, který není přidružen k ručně definované přenosové frontě klastru, je `CS.QM1`. Není přidružen k ručně definované přenosové frontě, protože žádný z názvů kanálů v atributu **CLCHNAME** přenosových front neodpovídá `CS.QM1`.



Obrázek 37. Priorita odesílacího kanálu přenosové fronty/klastru

Výběr ručně definovaných přenosových front podle odesílacích kanálů klastru

Ručně definovaná fronta má atribut přenosové fronty **USAGE** nastavený na hodnotu `XMITQ`a atribut názvu kanálu klastru **CLCHNAME** nastavený na specifický nebo generický název kanálu.

Pokud se název v atributu fronty **CLCHNAME** shoduje s názvem odesílacího kanálu klastru, je kanál přidružen k frontě. Název je buď přesná shoda, pokud název neobsahuje žádné zástupné znaky, nebo nejlepší shoda, pokud název obsahuje zástupné znaky.

Pokud definice produktu **CLCHNAME** ve více přenosových frontách odpovídají stejnému odesílacímu kanálu klastru, definice se budou překrývat. Pro vyřešení nejednoznačnosti existuje pořadí přednosti mezi shodami. Přesné shody mají vždy přednost. Obrázek 37 na stránce 291 zobrazuje přidružení mezi přenosovými frontami a odesílacími kanály klastru. Černé šipky zobrazují skutečná přidružení a šedé šipky, potenciální přidružení. Pořadí přednosti přenosových front v produktu Obrázek 37 na stránce 291 je:

`XMITQ.CL1.QM1`
: Přenosová fronta `XMITQ.CL1.QM1` má atribut **CLCHNAME** nastaven na hodnotu `CL1.QM1`. Definice atributu **CLCHNAME** , `CL1.QM1`, nemá žádné zástupné znaky a má přednost před jinými atributy `CLCHNAME` definovanými v jiných přenosových frontách, které se shodují se zástupnými znaky. Správce front ukládá všechny zprávy klastru, které mají být přeneseny odesílacím kanálem klastru `CL1.QM1` do přenosové fronty `XMITQ.CL1.QM1` . Jedinou výjimkou je, pokud má více přenosových front nastaven atribut **CLCHNAME** na hodnotu `CL1.QM1`. V takovém případě správce front uloží zprávy pro odesílací kanál klastru `CL1.QM1` v libovolné z těchto front. Vybere frontu libovolně při spuštění kanálu. Při opětovném spuštění kanálu může vybrat jinou frontu.

`XMITQ.CL1`
: Přenosová fronta `XMITQ.CL1` má atribut **CLCHNAME** nastaven na hodnotu `CL1.*`. Definice atributu **CLCHNAME** , `CL1.*`, má jeden koncový zástupný znak, který odpovídá názvu libovolného odesílacího kanálu klastru, který začíná na `CL1.`. Správce front ukládá všechny zprávy klastru, které mají být přeneseny libovolným kanálem odesilatele klastru, jehož název začíná na `CL1.` v přenosové frontě `XMITQ.CL1`, pokud neexistuje přenosová fronta s konkrétnější shodou, například fronta `XMITQ.CL1.QM1`. Jeden koncový zástupný znak činí definici méně specifickou než definici bez

zástupných znaků a více specifickou než definici s více zástupnými znaky nebo zástupné znaky, které jsou následovány více koncovými znaky.

XMITQ.CL.QM
XMITQ.CL.QM je název přenosové fronty s atributem **CLCHNAME** nastaveným na CL*.QM*. Definice CL*.QM* má dvě zástupné znaky, které se shodují s názvem libovolného odesílacího kanálu klastru, který začíná na CL., a buď zahrnuje, nebo končí na QM. Shoda je méně specifická než shoda s jedním zástupným znakem.

SYSTEM.CLUSTER.TRANSMIT. *channelName*|QUEUE
Pokud žádná přenosová fronta nemá atribut **CLCHNAME** , který by odpovídal názvu odesílacího kanálu klastru, který má správce front použít, použije správce front výchozí přenosovou frontu klastru. Výchozí přenosovou frontou klastru je buď přenosová fronta klastru s jedním systémem, SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo přenosová fronta klastru systému, kterou vytvořil správce front pro specifický odesílací kanál klastru SYSTEM.CLUSTER.TRANSMIT. *channelName*. Výchozí fronta závisí na nastavení atributu **DEFXMITQ** správce front.

Tip: Pokud nemáte jasnou potřebu překrývajících se definic, vyhněte se jim, protože mohou vést ke komplikovaným konfiguracím, které jsou obtížně pochopitelné.

Jak proces přepnutí odesílacího kanálu klastru na jinou přenosovou frontu pracuje

Chcete-li změnit přidružení odesílacích kanálů klastru k přenosovým frontám klastru, změňte kdykoli parametr **CLCHNAME** libovolné přenosové fronty nebo parametr správce front **DEFCLXQ** . Nic se neděje okamžitě. Změny se projeví pouze při spuštění kanálu. Při spuštění zkontroluje, zda má pokračovat v předávání zpráv ze stejné přenosové fronty. Tři druhy změn mění přidružení odesílacího kanálu klastru k přenosové frontě.

1. Předefinování parametru **CLCHNAME** přenosové fronty, ke které je odesílací kanál klastru aktuálně přidružen, aby byla méně specifická nebo prázdná, nebo odstranění přenosové fronty klastru při zastavení kanálu.

   Některá jiná přenosová fronta klastru se nyní může lépe shodovat s názvem kanálu. Nebo pokud se žádné jiné přenosové fronty neshodují s názvem odesílacího kanálu klastru, musí se přidružení 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 lépe odpovídat odesílacímu kanálu klastru, než je přenosová fronta, ke které je aktuálně přidružen odesílací kanál klastru. Pokud je odesílací kanál klastru aktuálně přidružen k výchozí přenosové frontě klastru, může být přidružen k ručně definované přenosové frontě klastru.
3. Pokud je odesílací kanál klastru aktuálně přidružen k výchozí přenosové frontě klastru, změňte parametr správce front **DEFCLXQ** .

Pokud se změní přidružení odesílacího kanálu klastru, při spuštění kanálu se jeho přidružení přepne do nové přenosové fronty. Během přepnutí zajišťuje, že nebudou ztraceny žádné zprávy. Zprávy jsou přenášeny do nové přenosové fronty v pořadí, ve kterém by kanál přenesl zprávy do vzdáleného správce front.

Zapamatujte si: Společně s jakýmkoli postoupením zpráv v klastru musíte vložit zprávy do skupin, abyste se ujistili, že zprávy, které musí být doručeny, jsou doručeny v pořadí. Ve vzácných případech mohou být zprávy v klastru mimo pořadí.

Proces přepnutí prochází následujícími transakčními kroky. Dojde-li k přerušení procesu přepínače, bude aktuální transakční krok obnoven při opětovném spuštění kanálu.

Krok 1-Zpracovat zprávy z původní přenosové fronty
Odesílací kanál klastru je přidružen k nové přenosové frontě, kterou může sdílet s ostatními odesílacími kanály klastru. Zprávy pro odesílací kanál klastru jsou i nadále umístěny do původní přenosové fronty. Přechodný proces přepínače přenáší zprávy z původní přenosové fronty do nové přenosové fronty. Odesílací kanál klastru předává zprávy z nové přenosové fronty přijímacímu kanálu

klastru. Stav kanálu zobrazuje odesílací kanál klastru, který je stále přidružen ke staré přenosové frontě.

Proces přepínání pokračuje také v přenosu nově příchozích zpráv. Tento krok pokračuje, dokud počet zbývajících zpráv, které mají být postoupeny procesem přepínače, nedosáhne nuly. Když počet zpráv dosáhne nuly, procedura se přesune na krok 2.

Během kroku 1 se zvýší aktivita disku pro kanál. Trvalé zprávy jsou potvrzeny z první přenosové fronty a do druhé přenosové fronty. Tato disková aktivita je navíc k potvrzením zpráv při jejich umístění do přenosové fronty a jejich odebrání z přenosové fronty v rámci normálního přenosu zpráv. V ideálním případě během procesu přepínání nepřicházejí žádné zprávy, takže přechod může proběhnout co nejrychleji. Pokud zprávy dorazí, proces přepínače je zpracuje.

Krok 2-Zpracovat zprávy z nové přenosové fronty

Jakmile v původní přenosové frontě pro odesílací kanál klastru nezůstanou žádné zprávy, budou nové zprávy umístěny přímo do nové přenosové fronty. Stav kanálu zobrazuje, že kanál odesilatele klastru je přidružen k nové přenosové frontě. Do protokolu chyb správce front je zapsána následující zpráva: " AMQ7341 `Fronta přenosu pro kanál` *`ChannelName`* `je` *`QueueName`* ."

Atributy více přenosových front klastru a přenosových front klastru

Máte možnost volby předávání zpráv klastru různým správcům front, kteří ukládají zprávy do jedné přenosové fronty klastru, nebo do více front. U jedné fronty máte jednu sadu atributů přenosové fronty klastru pro nastavení a dotazování; u více front máte více sad. U některých atributů je výhodou mít více sad: například dotazování na hloubku fronty vám řekne, kolik zpráv čeká na předání jedním nebo sadou kanálů, spíše než všemi kanály. U jiných atributů je nevýhodou mít více sad: například pravděpodobně nebudete chtít konfigurovat stejná přístupová oprávnění pro každou přenosovou frontu klastru. Z tohoto důvodu jsou přístupová oprávnění vždy kontrolována podle profilu pro produkt `SYSTEM.CLUSTER.TRANSMIT.QUEUE`, a nikoli podle profilů pro konkrétní přenosovou frontu klastru. Chcete-li použít podrobnější kontroly zabezpečení, prohlédněte si téma Řízení přístupu a více přenosových front klastru.

Více odesílacích kanálů klastru a více přenosových front

Správce front ukládá zprávu do přenosové fronty klastru před jejím předáním do odesílacího kanálu klastru. Vybere odesílací kanál klastru, který je připojen k místu určení pro zprávu. Může mít možnost výběru odesílacích kanálů klastru, které se všechny připojují ke stejnému místu určení. Cílem může být stejná fyzická fronta připojená více odesílacími kanály klastru k jednomu správci front. Cílem může být také mnoho fyzických front se stejným názvem fronty, jejichž hostitelem je jiný správce front ve stejném klastru. V případě, že existuje volba odesílacích kanálů klastru připojených k místu určení, algoritmus vyrovnávání pracovní zátěže zvolí jeden z nich. Volba závisí na řadě faktorů; viz Algoritmus správy pracovní zátěže klastru.

V systémech Obrázek 38 na stránce 294, `CL1.QM1`, `CL1.QM2` a `CS.QM1` jsou všechny kanály, které mohou vést ke stejnému cíli. Pokud například definujete `Q1` v `CL1` on `QM1` a `QM2` pak `CL1.QM1` a `CL1.QM2` obě poskytují trasy do stejného místa určení, `Q1`, ve dvou různých správcích front. Pokud se kanál `CS.QM1` nachází také v `CL1`, je to také kanál, který může převzít zpráva pro `Q1` . Členství v klastru `CS.QM1` může být definováno pomocí seznamu názvů klastru, což je důvod, proč název kanálu neobsahuje název klastru ve své konstrukci. V závislosti na parametrech vyrovnávání pracovní zátěže a odesílající aplikaci mohou být některé zprávy pro produkt `Q1` umístěny v jednotlivých přenosových frontách, `XMITQ.CL1.QM1`, `XMITQ.CL1` a `SYSTEM.CLUSTER.TRANSMIT.CS.QM1`.

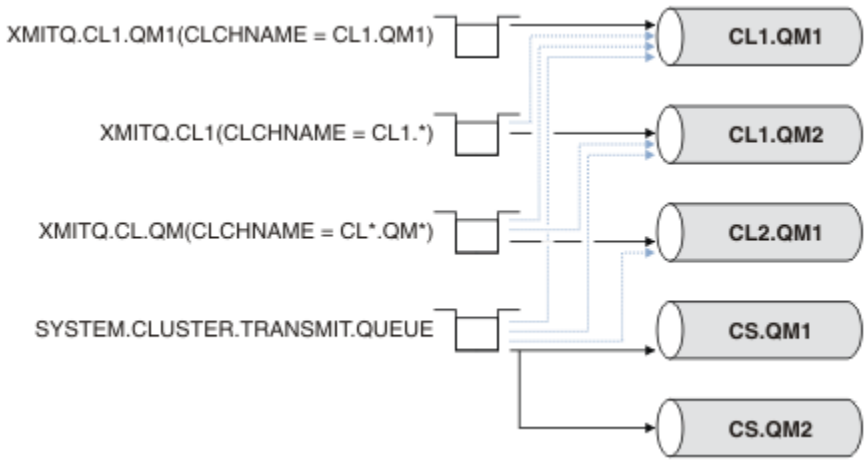
Máte-li v úmyslu oddělit provoz zpráv tak, aby zprávy pro stejné místo určení nesdílely fronty nebo kanály se zprávami pro různá místa určení, musíte nejprve zvážit, jak rozdělit provoz na různé odesílací kanály klastru a poté jak oddělit zprávy pro konkrétní kanál na jinou přenosovou frontu. Fronty klastru ve stejném klastru, ve stejném správci front, obvykle sdílejí stejné kanály klastru. Samotná definice více přenosových front klastru nestačí k oddělení provozu zpráv klastru do různých front. Pokud neoddělíte zprávy pro různé cílové fronty na různé kanály, budou zprávy sdílet stejnou přenosovou frontu klastru.

Přímým způsobem, jak oddělit kanály, které zprávy používají, je vytvořit více klastrů. V každém správci front v každém klastru definujte pouze jednu frontu klastru. Pokud pak pro každou kombinaci klastru

a správce front definujete jiný přijímací kanál klastru, nebudou zprávy pro každou frontu klastru sdílet kanál klastru se zprávami pro jiné fronty klastru. Pokud definujete oddělené přenosové fronty pro kanály klastru, odesílající správce front uloží 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 do různých správců front ve stejném klastru.

Volba přenosové fronty klastru neovlivňuje algoritmus vyrovnávání pracovní zátěže. Algoritmus vyrovnávání pracovní zátěže zvolí, který odesílací kanál klastru bude předávat zprávu. Umístí zprávu do přenosové fronty, která je obsluhována tímto kanálem. Je-li vyzván algoritmus vyrovnávání pracovní zátěže k opětovnému výběru, například pokud se kanál zastaví, může být schopen vybrat jiný kanál pro postoupení zprávy. Pokud zvolí jiný kanál a nový kanál postoupí zprávy z jiné přenosové fronty klastru, algoritmus vyrovnávání pracovní zátěže přenese zprávu do jiné přenosové fronty.

V produktu Obrázek 38 na stránce 294jsou k výchozí přenosové frontě systému přidruženy dva odesílací kanály klastru `CS.QM1` a `CS.QM2`. Pokud algoritmus vyrovnávání pracovní zátěže ukládá zprávu v systému `SYSTEM.CLUSTER.TRANSMIT.QUEUE`nebo v jiné přenosové frontě klastru, je název odesílacího kanálu klastru, který má zprávu předat, uložen v ID korelace zprávy. Každý kanál předává pouze ty zprávy, které odpovídají ID korelace s názvem kanálu.



Obrázek 38. Více odesílacích kanálů klastru

Pokud se produkt `CS.QM1` zastaví, budou prozkoumány zprávy v přenosové frontě pro tento odesílací kanál klastru. Zprávy, které mohou být předány jiným kanálem, jsou znovu zpracovány algoritmem vyrovnávání pracovní zátěže. Jejich ID korelace je resetováno na alternativní název odesílacího kanálu klastru. Pokud je alternativní kanál odesilatele klastru `CS.QM2`, zpráva zůstane v systému `SYSTEM.CLUSTER.TRANSMIT.QUEUE`. Je-li alternativním kanálem `CL1.QM1`, algoritmus vyrovnávání pracovní zátěže přenese zprávu do adresáře `XMITQ.CL1.QM1`. Při restartování kanálu odesilatele klastru jsou nové zprávy a zprávy, které nebyly označeny pro jiný kanál odesilatele klastru, znovu přeneseny kanálem.

Můžete změnit přidružení mezi přenosovými frontami a odesílacími kanály klastru na spuštěném systému. Můžete změnit parametr **CLCHNAME** v přenosové frontě nebo změnit parametr správce front **DEFCLXQ** . Když se kanál, který je ovlivněn změnou, restartuje, spustí proces přepínání přenosové fronty; viz “Jak proces přepnutí odesílacího kanálu klastru na jinou přenosovou frontu pracuje” na stránce 292.

Proces přepnutí přenosové fronty se spustí po restartování kanálu. Proces opětovného vyvážení pracovní zátěže se spustí při zastavení kanálu. Oba procesy mohou být spuštěny paralelně.

Jednoduchý případ je, když zastavení odesílacího kanálu klastru nezpůsobí, že proces nového vyvážení změní odesílací kanál klastru, který má předávat zprávy ve frontě. V tomto případě nemůže žádný jiný odesílací kanál klastru předávat zprávy do správného místa určení. Pokud není k dispozici žádný alternativní odesílací kanál klastru pro přesměrování zpráv do místa určení, zůstanou zprávy po zastavení odesílacího kanálu klastru označeny pro stejný odesílací kanál klastru. Je-li při spuštění kanálu přepínač nevyřízený, procesy přepínání přesunou zprávy do jiné přenosové fronty, kde jsou zpracovány stejným kanálem odesilatele klastru.

Složitějším případem je situace, kdy více než jeden odesílací kanál klastru může zpracovat některé zprávy do stejného místa určení. Zastavíte a restartujete odesílací kanál klastru, abyste spustili přepínač přenosové fronty. V mnoha případech při restartování kanálu již algoritmus vyrovnávání pracovní zátěže přesunul zprávy z původní přenosové fronty do různých přenosových front obsluhovaných různými odesílacími kanály klastru. Pouze ty zprávy, které nemohou být předány jiným kanálem odesilatele klastru, zůstávají převedeny do nové přenosové fronty. V některých případech, pokud je kanál rychle restartován, některé zprávy, které by mohly být přeneseny algoritmem vyrovnávání pracovní zátěže, zůstávají. V takovém případě jsou některé zbývající zprávy přepínány procesem vyrovnávání pracovní zátěže a některé procesem přepínání přenosové fronty.

Související pojmy

Kanály klastru

Klastrování: Izolace aplikace pomocí více přenosových front klastru

"Výpočet velikosti protokolu" na stránce 628
Odhad velikosti protokolu, který správce front potřebuje.

Související úlohy

Klastrování: Plánování konfigurace přenosových front klastru

"Vytvoření dvou překrývajících se klastrů se správcem front brány" na stránce 331
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 310
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

"Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 338
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další přenosovou frontu klastru k oddělení přenosu zpráv do jednoho správce front v klastru.

"Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaných ze správce front brány" na stránce 341
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další klastr k izolaci zpráv do konkrétní fronty klastru.

Vytvoření komunikace v klastru

Ke spuštění komunikačního kanálu je třeba iniciátor kanálu, pokud existuje zpráva, která má být doručena. Modul listener kanálu čeká na spuštění druhého konce kanálu, aby obdržel zprávu.

Než začnete

Chcete-li navázat komunikaci mezi správci front v klastru, konfigurujte propojení pomocí jednoho z podporovaných komunikačních protokolů. Podporované protokoly jsou:

- TCP nebo LU 6.2 na libovolné platformě
- Windows NetBIOS nebo SPX na systémech Windows

V rámci této konfigurace potřebujete také iniciátory kanálů a moduly listener kanálů, stejně jako v případě distribuovaného řazení do front.

Informace o této úloze

Všichni správci front klastru potřebují iniciátor kanálu k monitorování inicializační fronty definované systémem 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 listeneru kanálu čeká na příchozí síťové požadavky a v případě potřeby spustí příslušný přijímací kanál. Implementace modulů listener kanálu je specifická pro konkrétní platformu, existují však některé společné funkce.

Na všech platformách IBM MQ lze modul listener spustit pomocí příkazu **START LISTENER** .

Multi Na platformě Multiplatforms můžete spustit modul listener automaticky současně se správcem front. Chcete-li spustit modul listener automaticky, nastavte atribut CONTROL objektu LISTENER na hodnotu QMGR nebo STARTONLY.

z/OS Pro kanály CLUSRCVR v systému z/OS a pro kanály CLUSSDR v systému z/OSmusí být použit nesdílený port modulu listener (INDISP (QMGR)).

Postup

1. Spusťte inicializátor kanálu.
   - z/OS V systému z/OSexistuje jeden inicializátor kanálu pro každého správce front a je spuštěn jako samostatný adresní prostor. Spustíte jej pomocí příkazu **MQSC** START CHINIT , který zadáte jako součást spuštění správce front.
   - ALW Pokud je v systému AIX, Linux, and Windowspři spuštění správce front atribut správce front SCHINIT nastaven na hodnotu QMGR, iniciátor kanálu se automaticky spustí. Jinak jej lze spustit pomocí příkazu **runmqsc** START CHINIT nebo řídicího příkazu **runmqchi** .
   - IBM i Pokud je v systému IBM ipři spuštění správce front atribut správce front SCHINIT nastaven na hodnotu QMGR, iniciátor kanálu se automaticky spustí. Jinak jej lze spustit pomocí příkazu **runmqsc** START CHINIT nebo řídicího příkazu **runmqchi** .
2. Spusťte modul listener kanálu.
   - z/OS V systému z/OSpoužijte program listeneru kanálu poskytovaný produktem IBM MQ. Chcete-li spustit modul listener kanálu IBM MQ , použijte příkaz **MQSC** START LISTENER, který zadáte jako součást spuštění inicializátoru kanálu. Příklad:

     ```
     START LISTENER PORT(1414) TRPTYPE(TCP)
     ```

     nebo:

     ```
     START LISTENER LUNAME(LONDON.LUNAME) TRPTYPE(LU62)
     ```

     Členové skupiny sdílení front mohou místo modulu listener pro každého správce front používat sdílený modul listener. Nepoužívejte sdílené moduly listener s klastry. Konkrétně neuvádějte CONNAME kanálu CLUSRCVR jako adresu sdíleného modulu listener skupiny sdílení front. Pokud tak učiníte, správci front mohou přijímat zprávy pro fronty, pro které nemají definici.
   - IBM i V systému IBM ipoužijte program listeneru kanálu poskytovaný produktem IBM MQ. Chcete-li spustit modul listener kanálu IBM MQ , použijte příkaz **CL** STRMQMLSR. Příklad:

     ```
     STRMQMLSR MQMNAME(QM1) PORT(1414)
     ```

   - Windows V systému Windowspoužijte buď program listeneru kanálu poskytovaný produktem IBM MQ, nebo prostředky poskytované operačním systémem.

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

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

- Linux AIX V systému AIX and Linuxpoužijte buď program listeneru kanálu poskytovaný produktem IBM MQ, nebo prostředky poskytované operačním systémem; například **inetd** pro komunikaci TCP.

  Chcete-li spustit modul listener kanálu IBM 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 superuživatel nebo uživatel root. Pokud v souboru není následující řádek, přidejte jej podle obrázku:

  ```
  MQSeries    1414/tcp   # WebSphere MQ channel listener
  ```

  kde 1414 je číslo portu požadované produktem IBM MQ. Můžete změnit číslo portu, ale musí odpovídat číslu portu uvedenému na odesílajícím konci.

  b. Upravte soubor `/etc/inetd.conf`. Pokud v tomto souboru nemáte následující řádek, přidejte jej tak, jak je zobrazeno:

  ```
  MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta
  -m queue.manager.name
  ```

  kde proměnná *MQ_INSTALLATION_PATH* je nahrazena adresářem vysoké úrovně, ve kterém je nainstalován produkt IBM MQ .

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

  AIX V systému AIX:

  ```
  refresh -s inetd
  ```

  Linux V systému Linux:

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

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

  b. Spusťte příslušný příkaz.

  Pro Linux:

  ```
  kill -1 inetd processid
  ```

Nastavení nového klastru

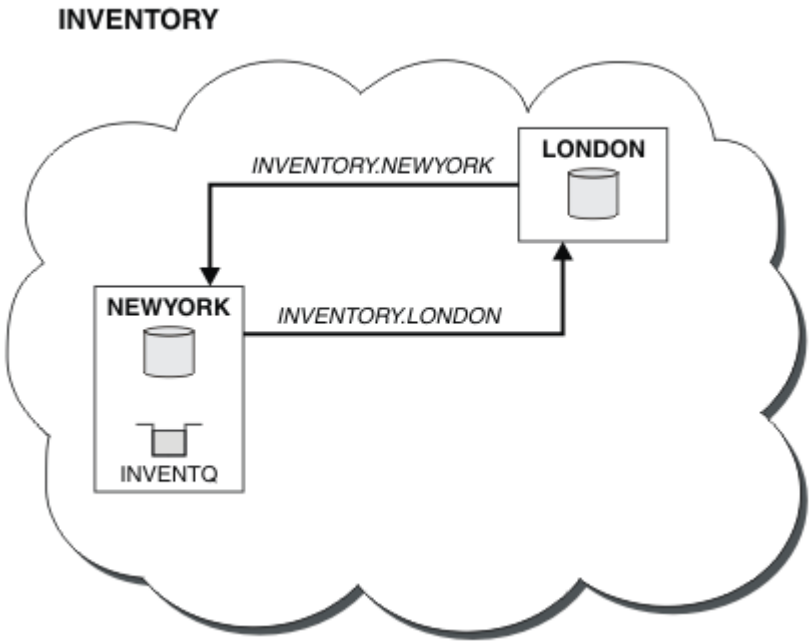
Postupujte podle těchto pokynů, abyste nastavili ukázkový klastr. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosovými frontami. Otestujte práci klastru odesláním zprávy z jednoho správce front do druhého.

Než začnete

- Místo toho, abyste dodržovali tyto pokyny, můžete použít jednoho z průvodců dodaných s produktem IBM MQ Explorer k vytvoření klastru, jako je klastr vytvořený touto úlohou. Klepněte pravým tlačítkem myši na složku Klastry správců front, poté klepněte na volbu **Nový** > **Klastr správců front**a postupujte podle pokynů uvedených v průvodci.
- Informace na pozadí, které vám pomohou porozumět krokům při nastavování klastru, viz “Definování front klastru” na stránce 285, Kanály klastru a Moduly listener.

Informace o této úloze

Nastavujete novou síť IBM MQ pro úložiště řetězců. Obchod má dvě pobočky, jednu v Londýně a jednu v New Yorku. Hostitelem dat a aplikací pro každé úložiště jsou systémy spouštějící samostatné správce front. Tito dva správci front se nazývají `LONDON` a `NEWYORK`. Aplikace inventáře je spuštěna v systému v New Yorku a je připojena ke správci front `NEWYORK`. Aplikace je řízena příchodem zpráv do fronty `INVENTQ` , jejímž hostitelem je `NEWYORK`. Oba správci front, `LONDON` a `NEWYORK`, mají být propojeni v klastru s názvem `INVENTORY` , aby mohli oba vložit zprávy do souboru `INVENTQ`.



Takto vypadá tento klastr:

Jednotlivé správce front v klastru můžete nakonfigurovat tak, aby odesílal zprávy jiným správcům front v klastru s použitím různých přenosových front klastru.

Pokyny pro nastavení klastru se trochu liší podle přenosového protokolu, počtu přenosových front nebo platformy. Máte na výběr ze tří kombinací. Ověřovací postup zůstává stejný pro všechny kombinace.

`INVENTORY` je malý klastr. Nicméně, to je užitečné jako důkaz konceptu. Důležité informace o tomto klastru jsou rozsah, který nabízí pro budoucí vylepšení.

Procedura

- “Nastavení klastru pomocí protokolu TCP/IP s jednou přenosovou frontou pro každého správce front” na stránce 299
- “Nastavení klastru v protokolu TCP/IP pomocí více přenosových front na jednoho správce front” na stránce 302
- “Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 304
- “Ověření klastru” na stránce 307

Související pojmy

Klastry

Porovnání klastrování a distribuovaného řazení do front

Komponenty klastru

Související úlohy

“Konfigurace klastru správců front” na stránce 284

Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

Nastavení klastru pomocí protokolu TCP/IP s jednou přenosovou frontou pro každého správce front

Toto je jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

Než začnete

Přehled vytvářeného klastru naleznete v části “Nastavení nového klastru” na stránce 297.

Atribut správce front **DEFCLXQ**musí být ponechán jako výchozí hodnota SCTQ.

Informace o této úloze

Chcete-li nastavit klastr v systému Multiplatforms pomocí přenosového protokolu TCP/IP, postupujte takto. z/OS V systému z/OSmusíte postupovat podle pokynů v části “Definování připojení TCP na systému z/OS” na stránce 971 , abyste nastavili připojení TCP/IP, místo abyste definovali listenery v kroku “4” na stránce 300. Jinak jsou kroky stejné pro z/OS, ale chybové zprávy se zapisují do konzoly a nikoli do protokolu chyb správce front.

Postup

1. Rozhodněte se o organizaci klastru a jeho názvu.

   Rozhodli jste se propojit dva správce front LONDON a NEWYORKs klastrem. Klastr s pouze dvěma správci front nabízí pouze okrajový přínos v síti, která má používat distribuované řazení do front. Je to dobrý způsob, jak začít a poskytuje prostor pro budoucí expanzi. Při otevírání nových větví úložiště můžete snadno přidávat nové správce front do klastru. Přidání nových správců front nenarušuje existující síť; viz “Přidání správce front do klastru” na stránce 308.

   V současné době je jedinou aplikací, kterou spouštíte, aplikace inventáře. Název klastru je INVENTORY.
2. Rozhodněte, kteří správci front mají uchovávat úplná úložiště.

   V libovolném klastru musíte určit alespoň jednoho správce front, nebo nejlépe dva, aby bylo možné uchovávat úplná úložiště. V tomto příkladu existují pouze dva správci front, LONDON a NEWYORK, kteří uchovávají úplná úložiště.

   a. Zbývající kroky můžete provést v libovolném pořadí.

   b. Při průchodu jednotlivými kroky mohou být do protokolu správce front zapsány varovné zprávy. Zprávy jsou výsledkem chybějících definic, které ještě musíte přidat.

   ```
   Examples of the responses to the commands are shown in a box
   like this after each step in this task.
   These examples show the responses returned by IBM MQ for AIX.
   The responses vary on other platforms.
   ```

   c. Před pokračováním v těchto krocích se ujistěte, že jsou spuštěni správci front.
3. Upravte definice správce front tak, aby přidávaly definice úložiště.

V každém správci front, který má obsahovat úplné úložiště, změňte definici lokálního správce front pomocí příkazu ALTER QMGR a zadejte atribut REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: IBM MQ queue manager changed.
```

Pokud například zadáte:

a. runmqsc LONDON

b. ALTER QMGR REPOS(INVENTORY)

LONDON se změní na úplné úložiště.

4. Definujte listenery.

   Definujte modul listener, který přijímá síťové požadavky od jiných správců front pro každého správce front v klastru. Ve správcích front LONDON zadejte následující příkaz:

   ```
   DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
   ```

   Atribut CONTROL zajišťuje, že se modul listener spustí a zastaví při spuštění správce front.

   Modul listener není při definování spuštěn, proto musí být poprvé ručně spuštěn pomocí následujícího příkazu MQSC:

   ```
   START LISTENER(LONDON_LS)
   ```

   Zadejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každého z nich.

   Existuje několik způsobů, jak tyto listenery definovat, jak ukazuje Listenery.

5. Definujte kanál CLUSRCVR pro správce front LONDON .

   V každém správci front v klastru definujete přijímací kanál klastru, na kterém může správce front přijímat zprávy. Viz Přijímací kanál klastru: CLUSRCVR . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, kde na něj mohou odkazovat jiní 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, na kterém je umístěn správce front, tj. LONDON.CHSTORE.COM. Síťovou adresu lze zadat jako alfanumerický název hostitele DNS nebo adresu IP v desítkovém formátu s tečkami IPv4 . Například 192.0.2.0nebo IPv6 hexadecimální formát; 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 systému z/OS, můžete vynechat CONNAME .

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
```

7. Definujte kanál CLUSSDR ve správci front LONDON .

   Ručně definujete kanál CLUSSDR z každého správce front úplného úložiště do každého jiného správce front úplného úložiště v klastru. Viz Kanál odesilatele klastru: CLUSSDR . V tomto případě existují pouze dva správci front, z nichž oba obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který odkazuje na kanál CLUSRCVR definovaný v druhém správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Pokud má správce front definice pro přijímací kanál klastru i odesílací kanál klastru ve stejném klastru, je kanál odesilatele 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 ve 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. Definovat frontu klastru INVENTQ

   Definujte frontu INVENTQ ve správci front NEWYORK a zadejte klíčové slovo 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 ostatním správcům front v klastru. Mohou do něj odesílat zprávy, aniž by pro něj museli vytvořit definici vzdálené fronty.

   Všechny definice jsou úplné. Na všech platformách spusťte program listener pro každého správce front. Program modulu listener čeká na příchozí síťové požadavky a spustí přijímací kanál klastru v případě potřeby.

Jak pokračovat dále

Nyní jste připraveni ověřit klastr.

Související úlohy

“Nastavení klastru v protokolu TCP/IP pomocí více přenosových front na jednoho správce front” na stránce 302

Toto je jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

“Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 304

Toto je jedno z témat stromu popisujících různé konfigurace pro jednoduchý klastr.

Nastavení klastru v protokolu TCP/IP pomocí více přenosových front na jednoho správce front

Toto je jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

Než začnete

Přehled vytvářeného klastru naleznete v části “Nastavení nového klastru” na stránce 297.

Informace o této úloze

Chcete-li nastavit klastr v systému Multiplatforms pomocí přenosového protokolu TCP/IP, postupujte takto. Správci front úložiště jsou konfigurováni tak, aby k odesílání zpráv mezi sebou a ostatními správci front v klastru používali jinou přenosovou frontu klastru. Pokud do klastru přidáte správce front, kteří mají také používat různé přenosové fronty, postupujte podle úlohy “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 310.

Postup

1. Rozhodněte se o organizaci klastru a jeho názvu.

   Rozhodli jste se propojit dva správce front LONDON a NEWYORKs klastrem. Klastr s pouze dvěma správci front nabízí pouze okrajový přínos v síti, která má používat distribuované řazení do front. Je to dobrý způsob, jak začít a poskytuje prostor pro budoucí expanzi. Při otevírání nových větví úložiště můžete snadno přidávat nové správce front do klastru. Přidání nových správců front nenarušuje existující síť; viz “Přidání správce front do klastru” na stránce 308.

   V současné době je jedinou aplikací, kterou spouštíte, aplikace inventáře. Název klastru je INVENTORY.

2. Rozhodněte, kteří správci front mají uchovávat úplná úložiště.

   V libovolném klastru musíte určit alespoň jednoho správce front, nebo nejlépe dva, aby bylo možné uchovávat úplná úložiště. V tomto příkladu existují pouze dva správci front, LONDON a NEWYORK, kteří uchovávají úplná úložiště.

   a. Zbývající kroky můžete provést v libovolném pořadí.

   b. Při průchodu jednotlivými kroky mohou být do protokolu správce front zapsány varovné zprávy. Zprávy jsou výsledkem chybějících definic, které ještě musíte přidat.

   ```
   Examples of the responses to the commands are shown in a box
   like this after each step in this task.
   These examples show the responses returned by IBM MQ for AIX.
   The responses vary on other platforms.
   ```

   c. Před pokračováním v těchto krocích se ujistěte, že jsou spuštěni správci front.

3. Upravte definice správce front tak, aby přidávaly definice úložiště.

   V každém správci front, který má obsahovat úplné úložiště, změňte definici lokálního správce front pomocí příkazu ALTER QMGR a zadejte atribut REPOS :

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

   ```
   1 : ALTER QMGR REPOS(INVENTORY)
   AMQ8005: IBM MQ queue manager changed.
   ```

   Pokud například zadáte:

   a. `runmqsc LONDON`

   b. `ALTER QMGR REPOS(INVENTORY)`

LONDON se změní na úplné úložiště.

4. Upravte definice správce front tak, aby pro každý cíl vytvářily samostatné přenosové fronty klastru.

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

   U každého správce front, kterého přidáte do klastru, rozhodněte, zda chcete používat samostatné přenosové fronty. Viz témata “Přidání správce front do klastru” na stránce 308 a “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 310.

5. Definujte listenery.

   Definujte modul listener, který přijímá síťové požadavky od jiných správců front pro každého správce front v klastru. Ve správcích front LONDON zadejte následující příkaz:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
```

   Atribut CONTROL zajišťuje, že se modul listener spustí a zastaví při spuštění správce front.

   Modul listener není při definování spuštěn, proto musí být poprvé ručně spuštěn pomocí následujícího příkazu MQSC:

```
START LISTENER(LONDON_LS)
```

   Zadejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každého z nich.

   Existuje několik způsobů, jak tyto listenery definovat, jak ukazuje Listenery.

6. Definujte kanál CLUSRCVR pro správce front LONDON .

   V každém správci front v klastru definujete přijímací kanál klastru, na kterém může správce front přijímat zprávy. Viz Přijímací kanál klastru: CLUSRCVR . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, kde na něj mohou odkazovat jiní 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, na kterém je umístěn správce front, tj. LONDON.CHSTORE.COM. Síťovou adresu lze zadat jako alfanumerický název hostitele DNS nebo adresu IP v desítkovém formátu s tečkami IPv4 . Například 192.0.2.0nebo IPv6 hexadecimální formát; 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 systému z/OS, můžete vynechat CONNAME .

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
```

8. Definujte kanál CLUSSDR ve správci front LONDON .

Ručně definujete kanál CLUSSDR z každého správce front úplného úložiště do každého jiného správce front úplného úložiště v klastru. Viz Kanál odesilatele klastru: CLUSSDR . V tomto případě existují pouze dva správci front, z nichž oba obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který odkazuje na kanál CLUSRCVR definovaný v druhém správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Pokud má správce front definice pro přijímací kanál klastru i odesílací kanál klastru ve stejném klastru, je kanál odesilatele 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 ve 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. Definovat frontu klastru INVENTQ

    Definujte frontu INVENTQ ve správci front NEWYORK a zadejte klíčové slovo 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 ostatním správcům front v klastru. Mohou do něj odesílat zprávy, aniž by pro něj museli vytvořit definici vzdálené fronty.

    Všechny definice jsou úplné. Na všech platformách spusťte program listener pro každého správce front. Program modulu listener čeká na příchozí síťové požadavky a spustí přijímací kanál klastru v případě potřeby.

Jak pokračovat dále

Nyní jste připraveni ověřit klastr.

Související úlohy

“Nastavení klastru pomocí protokolu TCP/IP s jednou přenosovou frontou pro každého správce front” na stránce 299

Toto je jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

“Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 304

Toto je jedno z témat stromu popisujících různé konfigurace pro jednoduchý klastr.

Nastavení klastru pomocí LU 6.2 na systému z/OS

Toto je jedno z témat stromu popisujících různé konfigurace pro jednoduchý klastr.

Než začnete

Přehled vytvářeného klastru naleznete v části “Nastavení nového klastru” na stránce 297.

Postup

1. Rozhodněte se o organizaci klastru a jeho názvu.

   Rozhodli jste se propojit dva správce front LONDON a NEWYORKs klastrem. Klastr s pouze dvěma správci front nabízí pouze okrajový přínos v síti, která má používat distribuované řazení do front. Je to dobrý způsob, jak začít a poskytuje prostor pro budoucí expanzi. Při otevírání nových větví úložiště můžete snadno přidávat nové správce front do klastru. Přidání nových správců front nenarušuje existující síť; viz “Přidání správce front do klastru” na stránce 308.

   V současné době je jedinou aplikací, kterou spouštíte, aplikace inventáře. Název klastru je INVENTORY.
2. Rozhodněte, kteří správci front mají uchovávat úplná úložiště.

   V libovolném klastru musíte určit alespoň jednoho správce front, nebo nejlépe dva, aby bylo možné uchovávat úplná úložiště. V tomto příkladu existují pouze dva správci front, LONDON a NEWYORK, kteří uchovávají úplná úložiště.

   a. Zbývající kroky můžete provést v libovolném pořadí.

   b. Během provádění kroků mohou být do konzoly systému z/OS zapsány varovné zprávy. Zprávy jsou výsledkem chybějících definic, které ještě musíte přidat.

   c. Před pokračováním v těchto krocích se ujistěte, že jsou spuštěni správci front.
3. Upravte definice správce front tak, aby přidávaly definice úložiště.

   V každém správci front, který má obsahovat úplné úložiště, změňte definici lokálního správce front pomocí příkazu ALTER QMGR a zadejte atribut REPOS :

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

   ```
   1 : ALTER QMGR REPOS(INVENTORY)
   AMQ8005: IBM MQ queue manager changed.
   ```

   Pokud například zadáte:

   a. `runmqsc LONDON`

   b. `ALTER QMGR REPOS(INVENTORY)`

   LONDON se změní na úplné úložiště.
4. Definujte listenery.

   z/OS Viz Iniciátor kanálu na z/OS a “Příjem na LU 6.2” na stránce 975.

   Modul listener není při definování spuštěn, proto musí být poprvé ručně spuštěn pomocí následujícího příkazu MQSC:

   ```
   START LISTENER(LONDON_LS)
   ```

   Zadejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každého z nich.
5. Definujte kanál CLUSRCVR pro správce front LONDON .

   V každém správci front v klastru definujete přijímací kanál klastru, na kterém může správce front přijímat zprávy. Viz Přijímací kanál klastru: CLUSRCVR . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, kde na něj mohou odkazovat jiní 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 ve správci front LONDON .

   Ručně definujete kanál CLUSSDR z každého správce front úplného úložiště do každého jiného správce front úplného úložiště v klastru. Viz Kanál odesilatele klastru: CLUSSDR . V tomto případě existují pouze dva správci front, z nichž oba obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který odkazuje na kanál CLUSRCVR definovaný v druhém správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Pokud má správce front definice pro přijímací kanál klastru i odesílací kanál klastru ve stejném klastru, je kanál odesilatele 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 ve 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. Definovat frontu klastru INVENTQ

   Definujte frontu INVENTQ ve správci front NEWYORK a zadejte klíčové slovo 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 ostatním správcům front v klastru. Mohou do něj odesílat zprávy, aniž by pro něj museli vytvořit definici vzdálené fronty.

   Všechny definice jsou úplné. Na všech platformách spusťte program listener pro každého správce front. Program modulu listener čeká na příchozí síťové požadavky a spustí přijímací kanál klastru v případě potřeby.

Jak pokračovat dále

Nyní jste připraveni ověřit klastr.

Související úlohy

“Nastavení klastru pomocí protokolu TCP/IP s jednou přenosovou frontou pro každého správce front” na stránce 299
Toto je jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

“Nastavení klastru v protokolu TCP/IP pomocí více přenosových front na jednoho správce front” na stránce 302
Toto je jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

Ověření klastru

Témata typu peer popisují tři různé konfigurace pro jednoduchý klastr. Toto téma vysvětluje, jak ověřit klastr.

Než začnete

Toto téma předpokládá, že ověřujete klastr, který jste vytvořili pomocí jedné z následujících úloh:

- “Nastavení klastru pomocí protokolu TCP/IP s jednou přenosovou frontou pro každého správce front” na stránce 299.
- “Nastavení klastru v protokolu TCP/IP pomocí více přenosových front na jednoho správce front” na stránce 302.
- “Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 304.

Přehled klastru, který byl vytvořen, naleznete v části “Nastavení nového klastru” na stránce 297.

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, abyste odeslali zprávu požadavku do fronty klastru a odpověděli zprávou odpovědi do neklastrované fronty odpovědí.

Postup

Zadáním příkazů produktu DISPLAY **runmqsc** ověřte klastr.

Odpovědi, které vidíte, by měly být jako odpovědi v následujících krocích.

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)
```

Odesílejte zprávy mezi dvěma správci front pomocí funkce **amqsput**.

3. V systému LONDON spusťte příkaz **amqsput INVENTQ LONDON**.

   Zadejte některé zprávy následované prázdným řádkem.

4. V systému NEWYORK spusťte příkaz **amqsget INVENTQ NEWYORK**.

   Nyní se zobrazí zprávy, které jste zadali v systému LONDON. Po 15 sekundách program skončí.

Odesílejte zprávy mezi dvěma správci front pomocí vlastních programů.

V následujících krocích produkt LONDON vloží zprávu do INVENTQ at NEWYORK a obdrží odpověď do své fronty 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 zprávy na LONDON_reply.
   e) Zadejte volání MQPUT pro vložení zprávy.
   f) Potvrďte zprávu.
6. V systému NEWYORK přijměte 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) Vyvolejte volání MQGET a získejte zprávu z INVENTQ.
   d) Načtěte název *ReplyToQ* z deskriptoru zprávy.
   e) Do pole ObjectName deskriptoru objektu zadejte název *ReplyToQ* .
   f) Nastavte volby MQOPEN na hodnotu MQOO_OUTPUT.
   g) Zadejte MQOPEN volání k otevření LONDON_reply ve správci front LONDON.
   h) Zadejte volání MQPUT pro vložení zprávy do souboru LONDON_reply.
7. Na systému LONDON přijměte odpověď.
   a) Nastavte volby MQOPEN na hodnotu MQOO_BROWSE.
   b) Zadejte volání MQOPEN pro otevření fronty LONDON_reply.
   c) Zadejte volání MQGET , abyste získali zprávu z LONDON_reply.

Přidání správce front do klastru

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí jedné přenosové fronty klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY je nastaven podle popisu v části “Nastavení nového klastru” na stránce 297. Obsahuje dva správce front, LONDON a NEWYORK, které obsahují úplná úložiště.
- Vlastníkem správce front PARIS je primární instalace. Pokud tomu tak není, musíte spustit příkaz **setmqenv** , abyste nastavili příkazové prostředí pro instalaci, do které produkt PARIS patří.
- Konektivita TCP existuje mezi všemi třemi systémy a správce front je konfigurován s modulem listener TCP, který je spuštěn pod kontrolou správce front.

Informace o této úloze

1. V Paříži se nastavuje nová větev úložiště řetězců a vy chcete do klastru přidat správce front s názvem PARIS .
2. Správce front PARIS odesílá aktualizace inventáře do aplikace spuštěné v systému v New Yorku vložením zpráv do fronty INVENTQ .

Chcete-li přidat správce front do klastru, postupujte takto.

Postup

1. Nejprve rozhodněte, na které úplné úložiště PARIS odkazuje.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště, a tak sestavuje vlastní dílčí úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile je do klastru přidán nový správce front, okamžitě se dozví i o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu odkazujete PARIS na správce front LONDONčistě z geografických důvodů.

   Poznámka: Po spuštění správce front PARIS proveďte zbývající kroky v libovolném pořadí.
2. Definujte kanál CLUSRCVR ve správci front PARIS.

   Každý správce front v klastru musí definovat přijímací kanál klastru, na 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 inzeruje dostupnost správce front pro příjem zpráv od jiných správců front v klastru INVENTORY. Nevytvářet definice v jiných správcích front pro odesílací konec přijímacího kanálu klastru INVENTORY.PARIS. Ostatní definice se vytvoří automaticky, když je to potřeba. Viz Kanály klastru.
3. z/OS
   Spusťte inicializátor kanálu v systému IBM MQ for z/OS.
4. Definujte kanál CLUSSDR ve správci front PARIS.

   Přidáte-li do klastru správce front, který není úplným úložištěm, definujete pouze jeden kanál odesilatele klastru, který vytvoří počáteční připojení k úplnému úložišti. Viz Kanál odesilatele klastru: CLUSSDR .

   V systému PARISproveďte následující definici kanálu CLUSSDR s názvem INVENTORY.LONDON pro správce front se síťovou adresou LONDON.CHSTORE.COM.

   ```
   DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at LONDON')
   ```
5. Volitelné: Pokud přidáváte do klastru správce front, který byl dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující další kroky:

a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, kterého přidáváte.

Tento krok zastaví kanály klastru a poskytne vaší lokální mezipaměti klastru novou sadu pořadových čísel, která budou v rámci zbytku klastru aktuální.

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

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

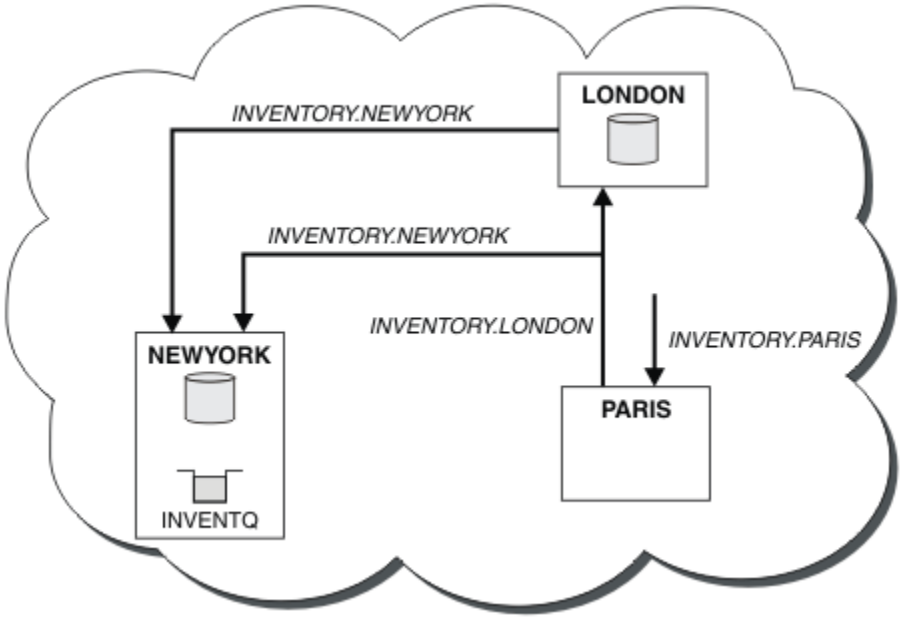
b) Restartovat kanál CLUSSDR

(například pomocí příkazu START CHANNEL).

c) Restartujte kanál CLUSRCVR.

Výsledky

Následující obrázek ukazuje klastr nastavený touto úlohou.



Obrázek 39. Klastr INVENTORY se třemi správci front

Po vytvoření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR , jsme přidali správce front PARIS do klastru.

Nyní se správce front PARIS z úplného úložiště v adresáři LONDONdozví, že hostitelem fronty INVENTQ je správce front NEWYORK. Když se aplikace, jejímž hostitelem je systém 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, pokud je její název správce front zadán jako cílový správce front a je poskytnuta fronta pro odpovědi.

Přidání správce front do klastru: samostatné přenosové fronty

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

Než začnete

- Správce front není členem žádného klastru.

- Klastr existuje; existuje úplné úložiště, ke kterému se může tento správce front připojit přímo a které je k dispozici. Postup vytvoření klastru viz “Nastavení nového klastru” na stránce 297.

Informace o této úloze

Tato úloha je alternativou k úloze “Přidání správce front do klastru” na stránce 308, ve které přidáte správce front do klastru, který umístí zprávy klastru do jedné 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, je výchozí nastavení použít jednu přenosovou frontu. Použití samostatných přenosových front je výhodné, pokud chcete monitorovat provoz určený pro různé správce front a různé klastry. Také můžete chtít oddělit provoz do různých cílů, abyste dosáhli cílů izolace nebo výkonu.

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 pro odeslání zprávy správci front, vytvoří přenosovou frontu klastru. Přenosovou frontu používá pouze tento odesílací kanál klastru. Přenosová fronta je trvalá-dynamická. Vytvoří se z modelové fronty SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUEs názvem SYSTEM.CLUSTER.TRANSMIT.*ChannelName*.

   Upozornění: Používáte-li vyhrazenou hodnotu SYSTEM.CLUSTER.TRANSMIT.QUEUES se správcem front, který byl upgradován z verze produktu starší než IBM WebSphere MQ 7.5, ujistěte se, že má SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE volbu SHARE/NOSHARE nastavenou na hodnotu **SHARE**.
2. Nejprve rozhodněte, na které úplné úložiště PARIS odkazuje.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště, a tak sestavuje vlastní dílčí úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile je do klastru přidán nový správce front, okamžitě se dozví i o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu odkazujete PARIS na správce front LONDONčistě z geografických důvodů.

   Poznámka: Po spuštění správce front PARIS proveďte zbývající kroky v libovolném pořadí.
3. Definujte kanál CLUSRCVR ve správci front PARIS.

   Každý správce front v klastru musí definovat přijímací kanál klastru, na 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 inzeruje dostupnost správce front pro příjem zpráv od jiných správců front v klastru INVENTORY. Nevytvářet definice v jiných správcích front pro odesílací konec přijímacího kanálu klastru INVENTORY.PARIS. Ostatní definice se vytvoří automaticky, když je to potřeba. Viz Kanály klastru.
4. Definujte kanál CLUSSDR ve správci front PARIS.

Přidáte-li do klastru správce front, který není úplným úložištěm, definujete pouze jeden kanál odesilatele klastru, který vytvoří počáteční připojení k úplnému úložišti. Viz Kanál odesilatele klastru: CLUSSDR .

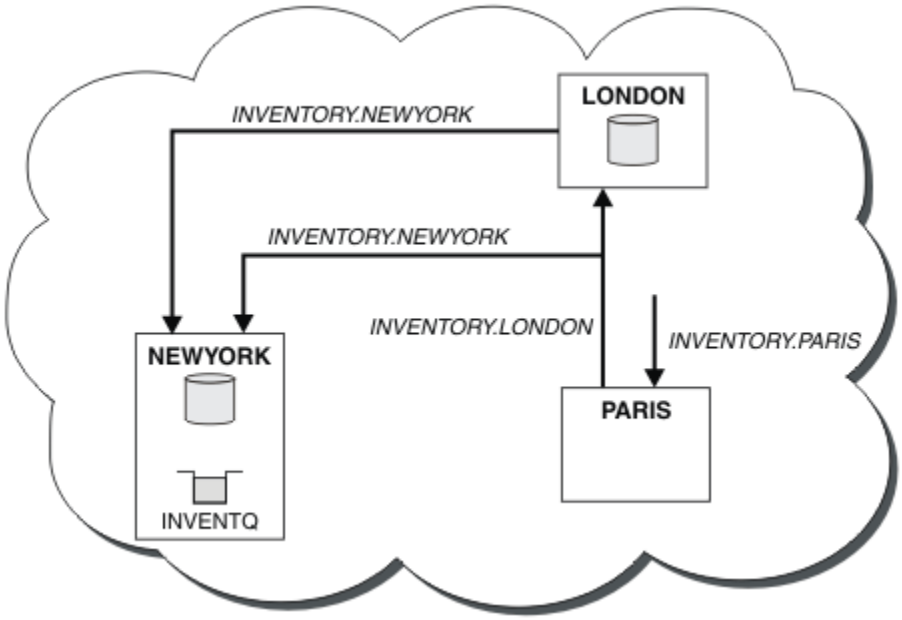
V systému PARISproveďte následující definici kanálu CLUSSDR s názvem INVENTORY.LONDON pro správce front se síťovou adresou LONDON.CHSTORE.COM.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at LONDON')
```

Správce front automaticky vytvoří trvalou přenosovou frontu dynamického klastru SYSTEM.CLUSTER.TRANSMIT.INVENTORY.LONDON z modelové fronty SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE. Nastaví atribut CLCHNAME přenosové fronty na hodnotu INVENTORY.LONDON.

Výsledky

Následující obrázek ukazuje klastr nastavený touto úlohou.



Obrázek 40. Klastr INVENTORY se třemi správci front

Po vytvoření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR , jsme přidali správce front PARIS do klastru.

Nyní se správce front PARIS z úplného úložiště v adresáři LONDONdozví, že hostitelem fronty INVENTQ je správce front NEWYORK. Když se aplikace, jejímž hostitelem je systém 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, pokud je její název správce front zadán jako cílový správce front a je poskytnuta fronta pro odpovědi.

Související pojmy

Jak vybrat typ přenosové fronty klastru, který se má použít

Související úlohy

Přidání správce front do klastru pomocí protokolu DHCP

Přidejte správce front do klastru pomocí protokolu DHCP. Úloha demonstruje vynechání hodnoty CONNAME v definici CLUSRCVR .

Přidání správce front do klastru pomocí protokolu DHCP

Přidejte správce front do klastru pomocí protokolu DHCP. Úloha demonstruje vynechání hodnoty CONNAME v definici CLUSRCVR .

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Úloha demonstruje dvě speciální funkce:

- Schopnost vynechat hodnotu CONNAME v definici CLUSRCVR .
- Schopnost použít +QMNAME+ na definici CLUSSDR .

V systému z/OSnení k dispozici žádná funkce.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Nastavení nového klastru” na stránce 297. Obsahuje dva správce front, LONDON a NEWYORK, které obsahují úplná úložiště.
- V Paříži se nastavuje nová větev úložiště řetězců a vy chcete do klastru přidat správce front s názvem PARIS .
- Správce front PARIS odesílá aktualizace inventáře do aplikace spuštěné v systému v New Yorku vložením zpráv do fronty INVENTQ.
- Mezi všemi třemi systémy existuje síťová konektivita.
- Síťový protokol je TCP.
- Systém správce front PARIS používá protokol DHCP, což znamená, že se adresy IP 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 systému LONDON.
- Administrátoři správce front PARIS nemají 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 takto.

Postup

1. Nejprve rozhodněte, na které úplné úložiště PARIS odkazuje.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště, a tak sestavuje vlastní dílčí úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile je do klastru přidán nový správce front, okamžitě se dozví i o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu se rozhodneme propojit PARIS se správcem front LONDONčistě z geografických důvodů.

   Poznámka: Po spuštění správce front PARIS proveďte zbývající kroky v libovolném pořadí.
2. Definujte kanál CLUSRCVR ve správci front PARIS.

   Každý správce front v klastru musí definovat přijímací kanál 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 inzeruje dostupnost správce front pro příjem zpráv od jiných správců front v klastru INVENTORY. V přijímacím kanálu klastru není třeba zadávat hodnotu CONNAME . Můžete

požádat produkt IBM MQ , abyste vyhledali název připojení ze systému, buď vynecháním volby CONNAME, nebo uvedením hodnoty CONNAME(' '). IBM MQ generuje hodnotu CONNAME pomocí aktuální adresy IP systému; viz CONNAME . Není třeba vytvářet definice v jiných správcích front pro odesílající konec přijímacího kanálu klastru INVENTORY.PARIS. Ostatní definice se vytvoří automaticky, když je to potřeba.

3. Definujte kanál CLUSSDR ve správci front PARIS.

   Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého počátečního úplného úložiště. V systému PARISvytvořte pro kanál s názvem INVENTORY.+QMNAME+ pro správce front následující definici se síťovou adresou 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 přidáváte do klastru správce front, který byl dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující další kroky:

   a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, kterého přidáváte.

      Tento krok zastaví kanály klastru a poskytne vaší lokální mezipaměti klastru novou sadu pořadových čísel, která budou v rámci zbytku klastru aktuální.

      ```
      REFRESH CLUSTER(INVENTORY) REPOS(YES)
      ```

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

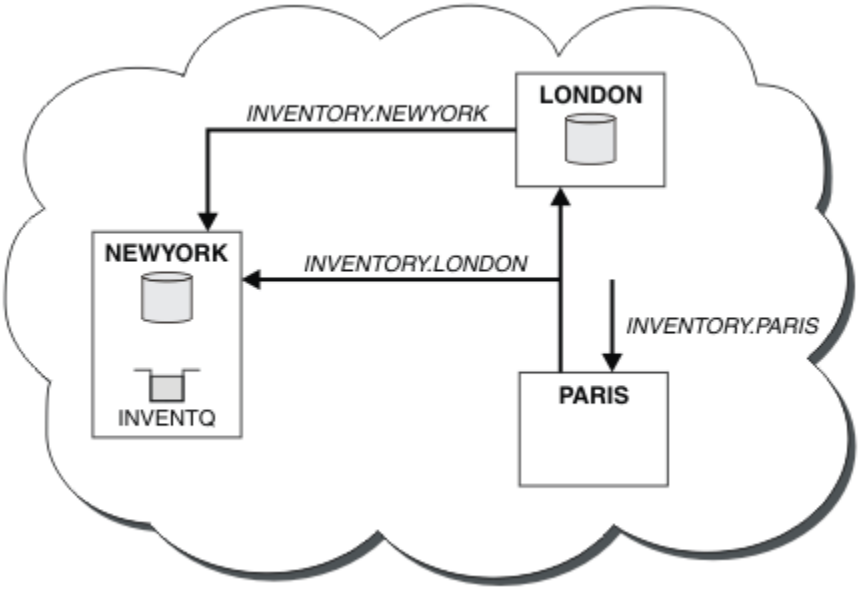
   b) Restartovat kanál CLUSSDR

      (například pomocí příkazu START CHANNEL).

   c) Restartujte kanál CLUSRCVR.

Výsledky

Klastr nastavený touto úlohou je stejný jako pro “Přidání správce front do klastru” na stránce 308:



Obrázek 41. Klastr INVENTORY se třemi správci front

Po vytvoření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR , jsme přidali správce front PARIS do klastru.

Ve správci front PARIS se spustí příkaz CLUSSDR obsahující řetězec +QMNAME+ . V LONDON systému IBM MQ přeloží soubor +QMNAME+ na název správce front (LONDON). IBM MQ pak odpovídá definici kanálu s názvem INVENTORY.LONDON odpovídající definici CLUSRCVR .

Produkt IBM MQ odešle zpět přeložený název kanálu do správce front PARIS . V systému PARISje definice kanálu CLUSSDR pro kanál s názvem INVENTORY.+QMNAME+ nahrazena interně generovanou definicí CLUSSDR pro systém INVENTORY.LONDON. Tato definice obsahuje vyřešený název kanálu, ale jinak je stejná jako definice +QMNAME+ , kterou jste provedli. Úložiště klastru jsou také aktuální 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 druhým.

Nyní se správce front PARIS z úložiště v adresáři LONDONdozví, že hostitelem fronty INVENTQ je správce front NEWYORK. Když se aplikace, jejímž hostitelem je systém 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, pokud je její název správce front zadán jako cílový správce front a je poskytnuta fronta pro odpovědi.

Související úlohy

Přidání správce front do klastru: samostatné přenosové fronty
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

Související odkazy

Definovat kanál

Přidání správce front, který je hostitelem fronty

Přidejte do klastru dalšího správce front, který bude hostitelem jiné fronty INVENTQ . Požadavky jsou odesílány střídavě do front v jednotlivých správcích front. V existujícím hostiteli INVENTQ není třeba provádět žádné změny.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Přidání správce front do klastru” na stránce 308. Obsahuje tři správce front: LONDON a NEWYORK obě obsahují úplná úložiště, PARIS obsahuje dílčí úložiště. Aplikace inventáře je spuštěna v systému v New Yorku a je připojena ke správci front NEWYORK . Aplikace je řízena příchodem zpráv do fronty INVENTQ .
- V Torontu je zřízen nový obchod. Chcete-li poskytnout další kapacitu, kterou chcete spustit aplikaci inventáře 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 přidat správce front s úplným úložištěm do klastru, postupujte podle pokynů v části “Přesunutí úplného úložiště do jiného správce front” na stránce 320.

Informace o této úloze

Chcete-li přidat správce front, který je hostitelem fronty, postupujte takto.

Postup

1. Nejprve rozhodněte, na které úplné úložiště TORONTO odkazuje.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště, a tak sestavuje vlastní dílčí úložiště. Úložiště, které zvolíte, nemá žádný zvláštní význam. V tomto příkladu zvolíme NEWYORK. Jakmile se nový správce front připojí ke klastru, komunikuje s oběma úložišti.
2. Definujte kanál CLUSRCVR .

   Každý správce front v klastru musí definovat přijímací kanál 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 TORONTO inzeruje svou dostupnost pro příjem zpráv od jiných správců front v klastru INVENTORY pomocí svého přijímacího kanálu 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 prvního úplného úložiště. V tomto případě vyberte volbu NEWYORK. Produkt TORONTO vyžaduje 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 přidáváte do klastru správce front, který byl dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující další kroky:
   a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, kterého přidáváte.

      Tento krok zastaví kanály klastru a poskytne vaší lokální mezipaměti klastru novou sadu pořadových čísel, která budou v rámci zbytku klastru aktuální.

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

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

b) Restartovat kanál CLUSSDR

(například pomocí příkazu START CHANNEL).

c) Restartujte kanál CLUSRCVR.

5. Zkontrolujte afinitu zpráv v aplikaci inventáře.

Než budete pokračovat, ujistěte se, že aplikace inventáře nemá žádné závislosti na posloupnosti zpracování zpráv a nainstalujte aplikaci na systém v Torontu.

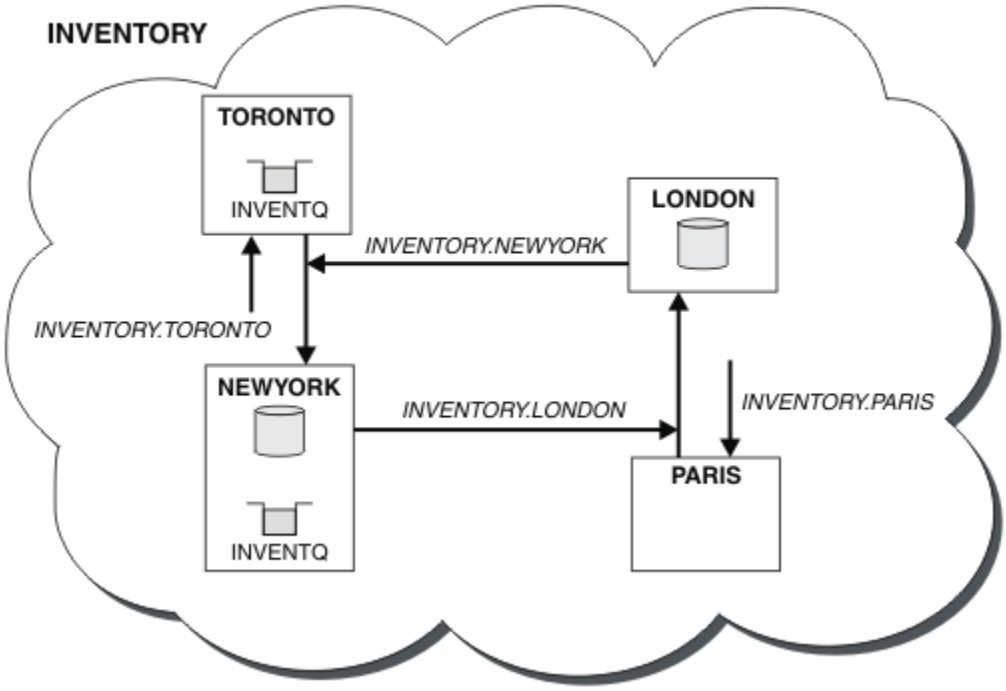
6. Definujte frontu klastru INVENTQ.

Hostitelem fronty INVENTQ , jejímž hostitelem je již správce front NEWYORK , bude také TORONTO. Definujte jej ve správci front TORONTO takto:

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

Výsledky

Obrázek 42 na stránce 317 zobrazuje klastr INVENTORY nastavený touto úlohou.



Obrázek 42. Klastr INVENTORY se čtyřmi správci front

Fronta INVENTQ a aplikace inventáře jsou nyní hostovány na dvou správcích front v klastru. To zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje rozdělit pracovní zátěž mezi dva správce front. Zprávy vkládané do souboru INVENTQ buď TORONTO , nebo NEWYORK jsou zpracovány instancí v lokálním správci front, kdykoli je to možné. Zprávy vkládané pomocí LONDON nebo PARIS jsou směrovány střídavě do TORONTO nebo NEWYORK, aby byla pracovní zátěž vyrovnaná.

Tato úprava klastru byla provedena bez nutnosti měnit definice ve správcích front NEWYORK, LONDONa PARIS. Úplná úložiště v těchto správcích front jsou automaticky aktualizována o informace, které potřebují k tomu, aby mohli odesílat zprávy na adresu INVENTQ na adrese TORONTO. Aplikace inventáře bude i nadále fungovat, pokud některý ze správců front NEWYORK nebo TORONTO nebude k dispozici a bude mít dostatečnou kapacitu. Aplikace inventáře musí být schopna pracovat správně, pokud je hostována v obou lokalitách.

Jak můžete vidět z výsledku této úlohy, můžete mít stejnou aplikaci spuštěnou ve více než jednom správci front. Můžete rovnoměrně rozdělit pracovní zátěž do klastrů.

Aplikace nemusí být schopna zpracovat záznamy v obou lokalitách. Předpokládejme například, že se rozhodnete přidat dotaz na zákaznický účet a aktualizovat aplikaci spuštěnou v adresáři LONDON a NEWYORK. Záznam účtu lze držet pouze na jednom místě. Můžete se rozhodnout řídit distribuci požadavků pomocí techniky dělení dat do oblastí. Distribuci záznamů můžete rozdělit. Můžete uspořádat polovinu záznamů, například pro čísla účtů 00000-49999, které mají být uchovávány v adresáři LONDON. Druhá polovina, v rozsahu 50000-99999 , je držena v NEWYORK. Poté můžete napsat uživatelský program pracovní zátěže klastru, abyste prozkoumali pole účtu ve všech zprávách a směrovali zprávy do příslušného správce front.

Jak pokračovat dále

Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte inicializátor kanálu na systému IBM MQ for z/OS. Na všech platformách spusťte program modulu listener ve správci front TORONTO. Program modulu listener čeká na příchozí síťové požadavky a spustí přijímací kanál klastru v případě potřeby.

z/OS Přidání skupiny sdílení front do existujících klastrů

Přidejte skupinu sdílení front v systému z/OS do existujících klastrů.

Než začnete

Poznámka:

1. Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.
2. Skupiny sdílení front jsou podporovány pouze v systému IBM MQ for z/OS. Tuto úlohu nelze použít pro jiné platformy.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Nastavení nového klastru” na stránce 297. Obsahuje dva správce front LONDON a NEWYORK.
- Chcete přidat skupinu sdílení front do tohoto klastru. Skupina QSGPse skládá ze tří správců front P1, P2a P3. Sdílejí instanci fronty INVENTQ , kterou má definovat P1.

Informace o této úloze

Chcete-li přidat nové správce front, kteří jsou hostiteli sdílené fronty, postupujte takto.

Postup

1. Rozhodněte, na které úplné úložiště správci front odkazují jako na první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště, a tak sestavuje vlastní dílčí úložiště. Není nijak důležité, které úplné úložiště si vyberete. V tomto příkladu vyberte volbu NEWYORK. Jakmile se skupina sdílení front připojí ke klastru, komunikuje s oběma úplnými úložišti.
2. Definujte kanály CLUSRCVR .

Každý správce front v klastru musí definovat přijímací kanál klastru, na kterém může přijímat zprávy. V systémech P1, P2a P3definujte:

```
DEFINE CHANNEL(INVENTORY.Pn) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(Pn.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-receiver channel for sharing queue manager')
```

Přijímací kanál klastru inzeruje dostupnost jednotlivých správců front pro příjem zpráv od jiných správců front v klastru INVENTORY.

3. Definujte kanál CLUSSDR pro skupinu sdílení front.

   Každý člen klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK. Jeden ze správců front ve skupině sdílení front potřebuje následující definici skupiny. Definice zajišťuje, že každý správce front má definici odesílacího kanálu klastru.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) QSGDISP(GROUP)
   DESCR('Cluster-sender channel to repository at NEWYORK')
   ```

4. Definujte sdílenou frontu.

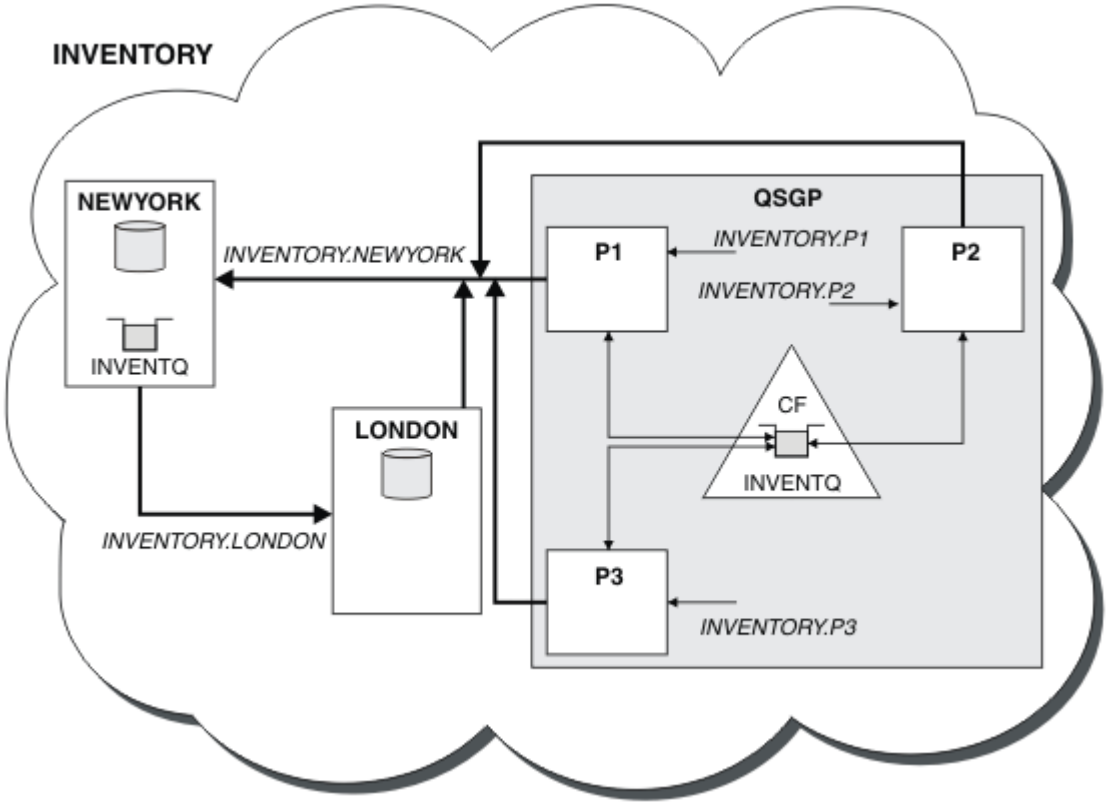
   Definujte frontu INVENTQ v systému P1 takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) QSGDISP(SHARED) CFSTRUCT(STRUCTURE)
   ```

   Spusťte inicializátor kanálu a program modulu listener pro nového správce front. Program listener naslouchá příchozím síťovým požadavkům a v případě potřeby spustí přijímací kanál klastru.

Výsledky

Obrázek 43 na stránce 319 zobrazuje klastr nastavený touto úlohou.



Obrázek 43. Klastr a skupina sdílení front

Nyní jsou zprávy vkládané do fronty INVENTQ pomocí LONDON směrovány střídavě kolem čtyř správců front, kteří jsou inzerováni jako hostitelci fronty.

Jak pokračovat dále

Výhodou členství ve skupině sdílení front v hostiteli fronty klastru je, že kterýkoli člen skupiny může odpovědět na požadavek. V tomto případě se produkt P1 stane nedostupným po přijetí zprávy ve sdílené frontě. Jiný člen skupiny sdílení front může místo toho odpovědět.

Přesunutí úplného úložiště do jiného správce front

Přesuňte úplné úložiště z jednoho správce front do jiného a sestavte nové úložiště z informací uchovávaných ve druhém úložišti.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Přidání správce front do klastru” na stránce 308.
- Z obchodních důvodů nyní chcete odebrat úplné úložiště ze správce front LONDONa nahradit je úplným úložištěm ve správci front PARIS. Správce front NEWYORK má pokračovat v zadržení úplného úložiště.

Informace o této úloze

Chcete-li přesunout úplné úložiště do jiného správce front, postupujte takto.

Postup

1. Změňte PARIS tak, aby se z něj udělal 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 ukazující na LONDON. Produkt LONDON již nemá obsahovat úplné úložiště pro klastr. PARIS musí mít nový odesílací kanál klastru, který ukazuje na NEWYORK, kde je nyní další 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 systému NEWYORK , který ukazuje na PARIS

   Aktuálně NEWYORK má odesílací kanál klastru ukazující na LONDON. Nyní, když se druhé úplné úložiště přesunulo do adresáře PARIS, musíte přidat nový odesílací kanál klastru na adrese NEWYORK , která 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 odesilatele klastru do PARIS, produkt PARIS se o klastru dozví z NEWYORK. Sestavuje vlastní úplné úložiště s použitím informací z webu NEWYORK.

4. Zkontrolujte, zda má správce front PARIS nyní úplné úložiště.

Zkontrolujte, zda správce front PARIS sestavil 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 systému NEWYORK.

Poznámka: Není-li správce front NEWYORK k dispozici, nelze toto sestavení informací dokončit. Nepřecházet na další krok, dokud nebude úloha dokončena.

5. Změnit definici správce front v systému LONDON

   Nakonec změňte správce front v adresáři LONDON tak, aby již neuchovoval úplné úložiště pro klastr. V systému LONDONzadejte příkaz:

   ```
   ALTER QMGR REPOS(' ')
   ```

   Správce front již nepřijímá žádné informace o klastru. Po 30 dnech vyprší platnost informací, které jsou uloženy v jejich úplném úložišti. Správce front LONDON nyní sestavuje vlastní dílčí úložiště.

6. Odeberte nebo změňte všechny nevyřízené definice.

   Pokud jste si jisti, že nové uspořádání klastru funguje podle očekávání, odeberte nebo změňte ručně definované definice CLUSSDR, které již nejsou správné.

   - Ve správci front PARIS musíte zastavit a odstranit odesílací kanál klastru do adresáře LONDONa poté zadat příkaz pro spuštění kanálu, aby klastr mohl znovu používat automatické kanály:

     ```
     STOP CHANNEL(INVENTORY.LONDON)
     DELETE CHANNEL(INVENTORY.LONDON)
     START CHANNEL(INVENTORY.LONDON)
     ```

   - Ve správci front NEWYORK musíte zastavit a odstranit odesílací kanál klastru do adresáře LONDONa poté zadat příkaz pro spuštění kanálu, aby klastr mohl znovu používat automatické kanály:

     ```
     STOP CHANNEL(INVENTORY.LONDON)
     DELETE CHANNEL(INVENTORY.LONDON)
     START CHANNEL(INVENTORY.LONDON)
     ```

   - Nahraďte všechny ostatní ručně definované odesílací kanály klastru, které ukazují na LONDON ve všech správcích front v klastru, kanály, které odkazují na NEWYORK nebo PARIS. Po odstranění kanálu vždy zadejte příkaz **start channel** , aby klastr mohl znovu používat automatické kanály. V tomto malém příkladu nejsou žádné další. Chcete-li zkontrolovat, zda existují další, které jste zapomněli, zadejte příkaz DISPLAY CHANNEL z každého správce front a zadejte hodnotu TYPE(CLUSSDR). Příklad:

     ```
     DISPLAY CHANNEL(*) TYPE(CLUSSDR)
     ```

   Je důležité, abyste tuto úlohu provedli co nejdříve po přesunutí úplného úložiště z adresáře LONDON do adresáře PARIS. V době před provedením této úlohy mohou správci front, kteří ručně definovali kanály CLUSSDR s názvem INVENTORY.LONDON , odesílat požadavky na informace prostřednictvím tohoto kanálu.

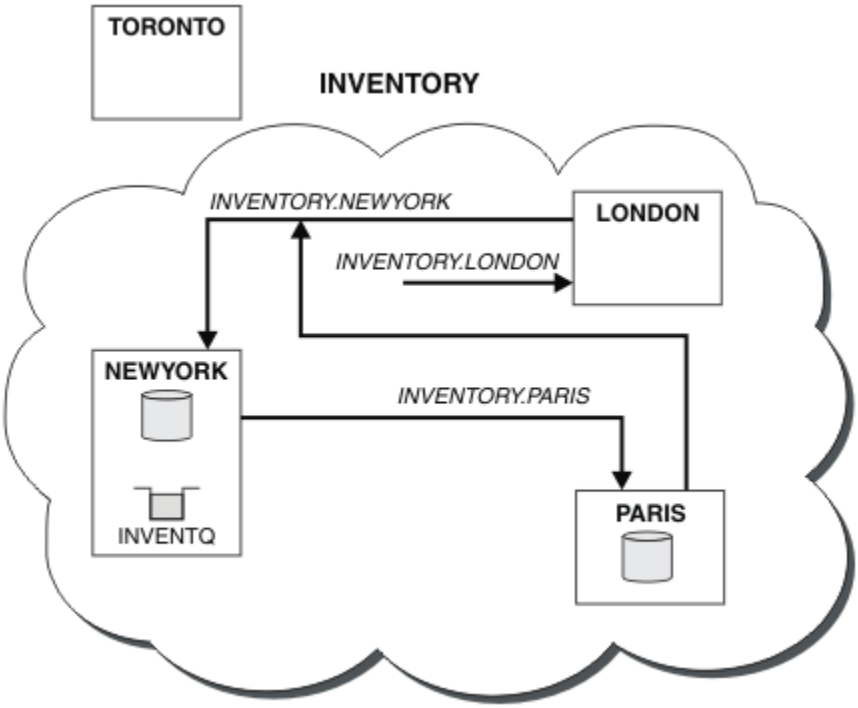
   Poté, co produkt LONDON přestane být úplným úložištěm, bude v případě, že takové požadavky obdrží, zapisovat chybové zprávy do svého protokolu chyb správce front. Následující příklady ukazují, které chybové zprávy se mohou zobrazit v systému LONDON:

   - 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 požadující informace od LONDON musí spoléhat na NEWYORK pro informace o klastru, dokud nebudou jejich ručně definované definice CLUSSDR opraveny tak, aby ukazovaly na PARIS. Tato situace nesmí být dlouhodobě tolerována jako platná konfigurace.

Výsledky

Obrázek 44 na stránce 322 zobrazuje klastr nastavený touto úlohou.



Obrázek 44. Klastr INVENTORY s úplným úložištěm přesunutým do umístění PARIS

Převod existující sítě na klastr

Převeďte existující síť distribuovaných front na klastr a přidejte dalšího správce front pro zvýšení kapacity.

Než začnete

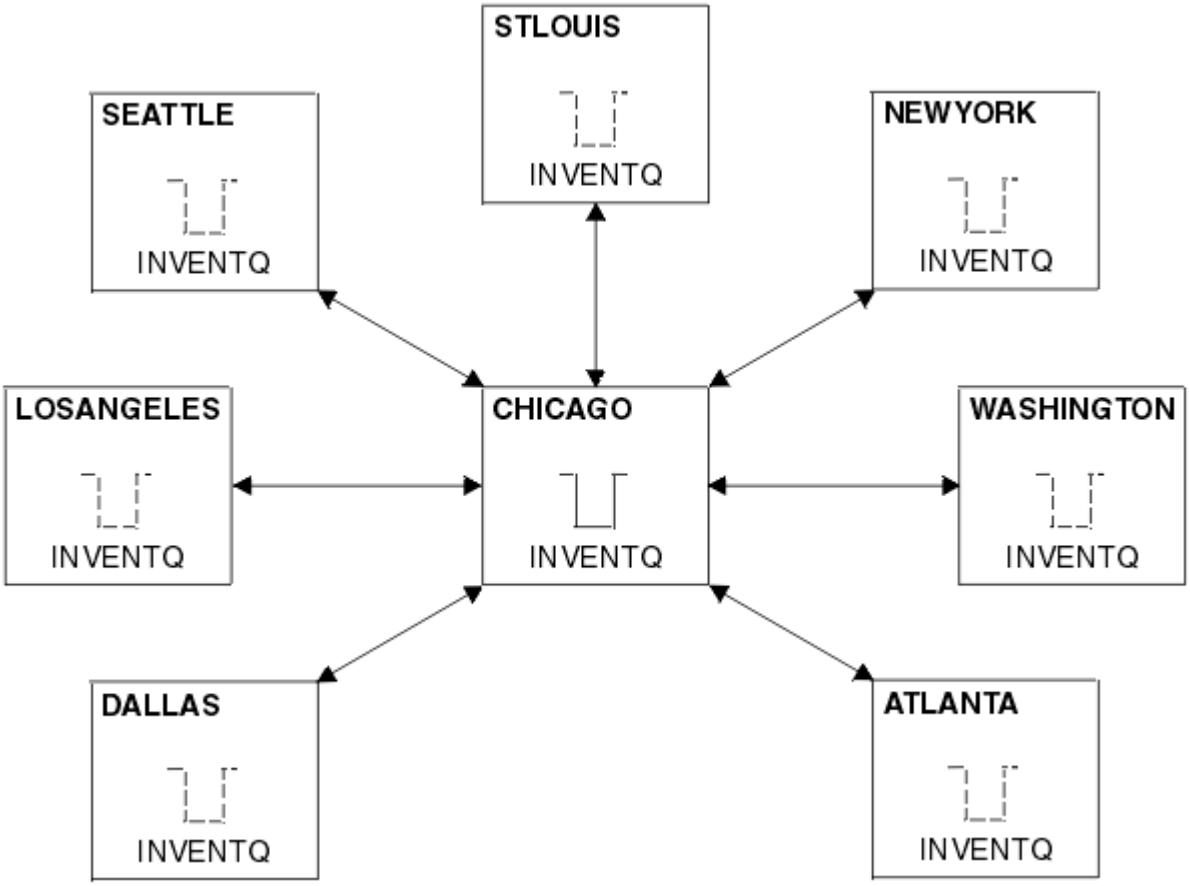
V "Nastavení nového klastru" na stránce 297 prostřednictvím "Přesunutí úplného úložiště do jiného správce front" na stránce 320 jste vytvořili a rozšířili nový klastr. Další dvě úlohy zkoumají jiný přístup: převod existující sítě správců front na klastr.

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Síť IBM MQ je již na místě a propojuje celostátní větve řetězového úložiště. Má rozbočovač a strukturu paprsků: všichni správci front jsou připojeni k jednomu centrálnímu správci front. Centrální správce front je v systému, v němž je spuštěna aplikace inventáře. Aplikace je řízena příchodem zpráv do fronty INVENTQ , pro kterou má každý správce front definici vzdálené fronty.

  Tato síť je znázorněna v souboru Obrázek 45 na stránce 323.



Obrázek 45. Rozbočovač a paprsková síť

- Chcete-li usnadnit administraci, převeďte tuto síť na klastr a na centrálním serveru vytvořte dalšího správce front pro sdílení pracovní zátěže.

  Název klastru je `CHNSTORE`.

  Poznámka: Název klastru `CHNSTORE` byl vybrán tak, aby umožňoval vytváření názvů přijímacích kanálů klastru pomocí názvů ve formátu *`cluster_name. queue_manager_name`* , které nepřesahují maximální délku 20 znaků, například `CHNSTORE.WASHINGTON`.
- Oba centrální správci front mají být hostiteli úplných úložišť a mají být přístupné pro aplikaci inventáře.
- Aplikace inventáře má být řízena příchodem zpráv do fronty `INVENTQ` , jejímž hostitelem je některý z centrálních správců front.
- Aplikace inventáře má být jedinou aplikací spuštěnou paralelně a přístupnou více než jedním správcem front. Všechny ostatní aplikace budou nadále spuštěny 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 takto.

Postup

1. Zkontrolujte afinitu zpráv v aplikaci inventáře.

   Než budete pokračovat, ujistěte se, že aplikace může zpracovat afinity zpráv. Afinity zpráv jsou vztahy mezi konverzačními zprávami, které jsou vyměňovány mezi dvěma aplikacemi, přičemž zprávy musí být zpracovány konkrétním správcem front nebo v určité posloupnosti. Další informace o afinitách zpráv viz: “Zpracování afinit zpráv” na stránce 398

2. Změňte dva centrální správce front tak, aby z nich měli správce front úplného úložiště.

   Dva správci front CHICAGO a CHICAGO2 jsou v centrálním serveru této sítě. Rozhodli jste se soustředit všechny aktivity přidružené ke klastru úložiště řetězu na tyto dva správce front. Kromě aplikace inventáře a definic pro frontu INVENTQ chcete, aby tito správci front hostili dvě úplná úložiště pro klastr. V každém ze dvou správců front zadejte následující příkaz:

   ```
   ALTER QMGR REPOS(CHNSTORE)
   ```

3. Definujte kanál CLUSRCVR pro každého správce front.

   U každého správce front v klastru definujte přijímací kanál klastru a odesílací kanál klastru. Nezáleží na tom, který kanál definujete jako první.

   Vytvořte definici CLUSRCVR pro inzerování každého správce front, jeho síťové adresy a dalších informací klastru. Například ve správci front ATLANTA:

   ```
   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 pro každého správce front definici CLUSSDR , aby bylo možné tohoto správce front propojit s jedním nebo více správci front úplného úložiště. Například můžete odkázat ATLANTA na 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 inventáře na CHICAGO2.

   Již máte aplikaci inventáře ve správci front 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 k dispozici 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 pomocí volby MAKEDEF funkce COMMAND příkazu **CSQUTIL** vytvořit přesnou kopii CHICAGO2 položky INVENTQ on CHICAGO.

   Když provedete tyto definice, odešle se zpráva do úplných úložišť v adresáři CHICAGO a CHICAGO2 a informace v nich obsažené se aktualizují. Správce front zjistí z úplných úložišť, když vloží zprávu do INVENTQ, že existuje výběr cílů pro zprávy.

7. Zkontrolujte, zda byly změny klastru šířeny.

   Zkontrolujte, zda definice, které jste vytvořili v předchozím kroku, byly šířeny prostřednictvím klastru. Zadejte následující příkaz pro správce front úplného úložiště:

   ```
   DIS QCLUSTER(INVENTQ)
   ```

Přidání nového, vzájemně propojeného klastru

Přidejte nový klastr, který sdílí některé správce front s existujícím klastrem.

Než začnete

Poznámka:

1. Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.
2. Před spuštěním této úlohy zkontrolujte kolize názvů front a pochopte důsledky. Než budete moci pokračovat, budete možná muset přejmenovat frontu nebo nastavit aliasy fronty.

Scénář:

- Klastr IBM MQ byl nastaven podle popisu v části “Převod existující sítě na klastr” na stránce 322.
- Má být implementován nový klastr s názvem MAILORDER . Tento klastr se skládá ze čtyř správců front, kteří jsou v klastru CHNSTORE ; CHICAGO, CHICAGO2, SEATTLEa ATLANTA, a dvou dalších správců front; HARTFORD a OMAHA. Aplikace MAILORDER je spuštěna v systému na adrese Omaha, který je připojen ke správci front OMAHA. Je řízen ostatními správci front v klastru, kteří vkládají zprávy do fronty MORDERQ .
- Úplná úložiště pro klastr MAILORDER jsou udržována ve dvou správcích front CHICAGO a CHICAGO2.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li přidat nový, propojený klastr, postupujte takto.

Postup

1. Vytvořte seznam názvů klastrů.

   Správci front úplného úložiště v adresáři CHICAGO a CHICAGO2 budou nyní uchovávat úplná úložiště pro oba klastry CHNSTORE a MAILORDER. Nejprve vytvořte seznam názvů obsahující názvy klastrů. Definujte seznam názvů v systémech CHICAGO a CHICAGO2takto:

   ```
   DEFINE NAMELIST(CHAINMAIL)
   DESCR('List of cluster names')
   NAMES(CHNSTORE, MAILORDER)
   ```

2. Změňte dvě definice správce front.

   Nyní změňte dvě definice správce front v adresáři CHICAGO a CHICAGO2. V současné době tyto definice ukazují, že správci front uchovávají úplná úložiště pro klastr CHNSTORE. Změňte tuto definici tak, aby ukazovala, že správci front uchovávají úplná úložiště pro všechny klastry uvedené v seznamu názvů CHAINMAIL . Změňte definice správce front CHICAGO a CHICAGO2 :

   ```
   ALTER QMGR REPOS(' ') REPOSNL(CHAINMAIL)
   ```

3. Změňte kanály CLUSRCVR na CHICAGO a CHICAGO2.

   Definice kanálů CLUSRCVR v CHICAGO a CHICAGO2 ukazují, že kanály jsou k dispozici v klastru CHNSTORE. Musíte změnit definici příjemce klastru tak, aby ukazovala, že kanály jsou k dispozici pro všechny klastry uvedené v seznamu názvů CHAINMAIL . Změňte definici příjemce klastru v adresáři CHICAGO:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSRCVR)
   CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

   V adresáři CHICAGO2zadejte příkaz:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSRCVR)
   CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

4. Změňte kanály CLUSSDR na systémech CHICAGO a CHICAGO2.

Změňte dvě definice kanálu CLUSSDR a přidejte seznam názvů. V adresáři CHICAGOzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

V adresáři CHICAGO2zadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

5. Vytvořte seznam názvů v adresáři SEATTLE a ATLANTA.

   Protože SEATTLE a ATLANTA budou členy více než jednoho klastru, musíte vytvořit seznam názvů obsahující názvy klastrů. Definujte seznam názvů v systémech SEATTLE a ATLANTAtakto:

   ```
   DEFINE NAMELIST(CHAINMAIL)
   DESCR('List of cluster names')
   NAMES(CHNSTORE, MAILORDER)
   ```

6. Změňte kanály CLUSRCVR na SEATTLE a ATLANTA.

   Definice kanálů CLUSRCVR v SEATTLE a ATLANTA ukazují, že kanály jsou k dispozici v klastru CHNSTORE. Změňte definice kanálu pro příjem klastru tak, aby ukazovaly, že kanály jsou k dispozici pro všechny klastry uvedené v seznamu názvů CHAINMAIL . V adresáři SEATTLEzadejte příkaz:

   ```
   ALTER CHANNEL(CHNSTORE.SEATTLE) CHLTYPE(CLUSRCVR)
   CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

   V adresáři ATLANTAzadejte příkaz:

   ```
   ALTER CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR)
   CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

7. Změňte kanály CLUSSDR na systémech SEATTLE a ATLANTA.

   Změňte dvě definice kanálu CLUSSDR a přidejte seznam názvů. V adresáři SEATTLEzadejte příkaz:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)
   CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

   V adresáři ATLANTAzadejte příkaz:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)
   CLUSTER(' ') CLUSNL(CHAINMAIL)
   ```

8. Definujte kanály CLUSRCVR a CLUSSDR na systémech HARTFORD a OMAHA.

   Ve dvou nových správcích front HARTFORD a OMAHAdefinujte kanály příjemce klastru a odesilatele klastru. Nezáleží na tom, v jakém pořadí definice provedete. V adresáři 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 adresáři 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 systému OMAHA.

   Posledním krokem k dokončení této úlohy je definování fronty MORDERQ ve správci front OMAHA. V adresáři OMAHAzadejte:

   ```
   DEFINE QLOCAL(MORDERQ) CLUSTER(MAILORDER)
   ```

10. Zkontrolujte, zda byly změny klastru šířeny.

    Zkontrolujte, zda definice, které jste vytvořili v předchozích krocích, byly šířeny prostřednictvím klastru. Zadejte následující příkazy pro správce front úplného úložiště:

    ```
    DIS QCLUSTER (MORDERQ)
    DIS CLUSQMGR
    ```

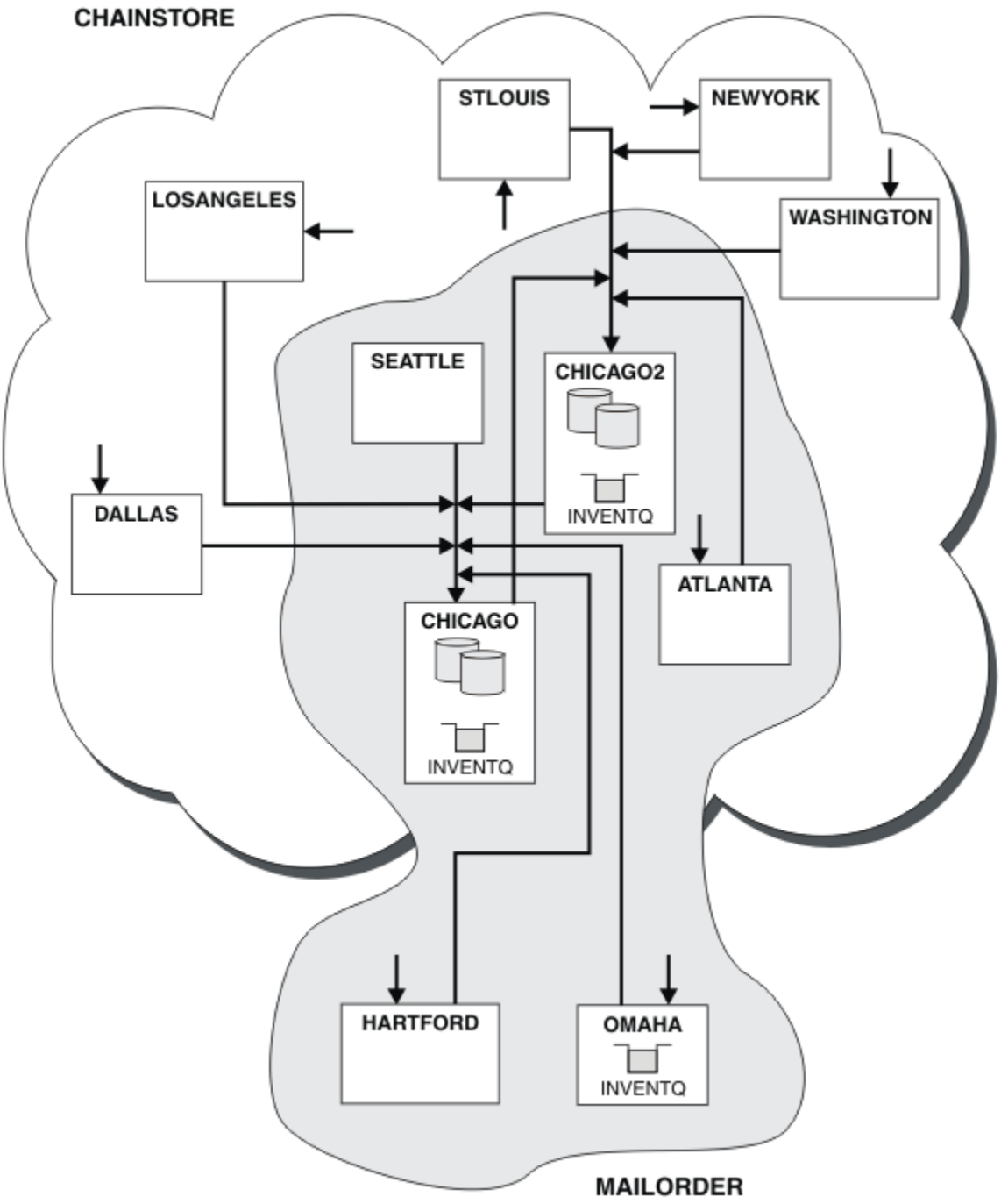
11.

Výsledky

Klastr nastavený touto úlohou je zobrazen v souboru Obrázek 46 na stránce 328.

Nyní máme dva překrývající se klastry. Úplná úložiště pro oba klastry jsou zadržena v adresáři CHICAGO a CHICAGO2. Aplikace objednávky pošty, která je spuštěna v systému OMAHA , je nezávislá na aplikaci inventáře, která běží v systému CHICAGO. Avšak někteří správci front, kteří jsou v klastru CHNSTORE , jsou také v klastru MAILORDER , a tak mohou odesílat zprávy do obou aplikací. Před provedením této úlohy, která má překrývat dva klastry, si uvědomte možnost kolizí názvů front.

Předpokládejme, že v systému NEWYORK v klastru CHNSTORE a v systému OMAHA v klastru MAILORDERexistuje fronta s názvem ACCOUNTQ. Pokud překrýváte klastry a poté aplikace v systému SEATTLE vloží zprávu do fronty ACCOUNTQ, může zpráva přejít na libovolnou instanci ACCOUNTQ.



Obrázek 46. Propojené klastry

Jak pokračovat dále

Předpokládejme, že se rozhodnete sloučit klastr `MAILORDER` s klastrem `CHNSTORE` a vytvořit jeden velký klastr s názvem `CHNSTORE`.

Chcete-li sloučit klastr `MAILORDER` s klastrem `CHNSTORE` tak, aby `CHICAGO` a `CHICAGO2` uchovaly úplná úložiště, postupujte takto:

- Pozměňte definice správce front pro CHICAGO a CHICAGO2, odeberte atribut REPOSNL, který určuje seznam názvů (CHAINMAIL), a nahraďte jej atributem REPOS, který určuje název klastru (CHNSTORE). Například:

```
ALTER QMGR(CHICAGO) REPOSNL(' ') REPOS(CHNSTORE)
```

- V každém správci front v klastru MAILORDER změňte všechny definice kanálů a definice front tak, aby se hodnota atributu CLUSTER změnila z MAILORDER na CHNSTORE. Například na adrese HARTFORDzadejte:

```
ALTER CHANNEL(MAILORDER.HARTFORD) CLUSTER(CHNSTORE)
```

  Do pole OMAHA zadejte:

```
ALTER QLOCAL(MORDERQ) CLUSTER(CHNSTORE)
```

- Změňte všechny definice, které určují seznam názvů klastrů CHAINMAIL, tj. definice kanálů CLUSRCVR a CLUSSDR v CHICAGO, CHICAGO2, SEATTLEa ATLANTA, tak, aby uváděli místo klastru CHNSTORE.

Z tohoto příkladu můžete vidět výhodu použití seznamů názvů. Namísto změny definic správců front pro položky CHICAGO a CHICAGO2 můžete změnit hodnotu seznamu názvů CHAINMAIL. Podobně namísto změny definic kanálů CLUSRCVR a CLUSSDR v definicích CHICAGO, CHICAGO2, SEATTLEa ATLANTAmůžete dosáhnout požadovaného výsledku změnou seznamu názvů.

Související úlohy

Odebrání sítě klastru

Odeberte klastr ze sítě a obnovte konfiguraci distribuovaných front.

Odebrání sítě klastru

Odeberte klastr ze sítě a obnovte konfiguraci distribuovaných front.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr IBM MQ byl nastaven podle popisu v části “Převod existující sítě na klastr” na stránce 322.
- Tento klastr má být nyní odebrán ze systému. Síť správců front bude i nadále fungovat tak, jak fungovala před implementováním klastru.

Informace o této úloze

Chcete-li odebrat síť klastru, postupujte takto.

Postup

1. Odeberte fronty klastru z klastru CHNSTORE .

   V systémech CHICAGO i CHICAGO2upravte definici lokální fronty pro frontu INVENTQ tak, aby byla fronta odebrána z klastru. Spusťte následující příkaz:

```
ALTER QLOCAL(INVENTQ) CLUSTER(' ')
```

   Při změně fronty jsou informace v úplných úložištích aktualizovány a šířeny v celém klastru. Aktivní aplikace používající 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 . Vrátí se kód příčiny MQRC_UNKNOWN_OBJECT_NAME .

Nejprve nemusíte provést krok 1, ale pokud ne, proveďte jej místo toho po kroku 4.

2. Zastavte všechny aplikace, které mají přístup ke frontě klastru.

   Zastavte všechny aplikace, které mají přístup k frontám klastru. Pokud tak neučiníte, některé informace o klastru mohou zůstat v lokálním správci front při aktualizaci klastru v kroku 5. Tyto informace se odeberou po zastavení všech aplikací a odpojení kanálů klastru.

3. Odeberte atribut úložiště ze správců front úplného úložiště.

   V systémech CHICAGO i CHICAGO2upravte definice správce front tak, aby byly odebrány atributy úložiště. Chcete-li to provést, zadejte příkaz:

   ```
   ALTER QMGR REPOS(' ')
   ```

   Správci front informují ostatní správce front v klastru, že již neuchovávají úplná úložiště. Když ostatní správci front obdrží tyto informace, zobrazí se zpráva s informací, že úplné úložiště bylo ukončeno. Zobrazí se také jedna nebo více zpráv, které označují, že pro klastr již nejsou k dispozici žádná úložiště CHNSTORE.

4. Odebrat kanály klastru.

   V systému 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 a poté příkaz CLUSRCVR . Nejprve nezadávejte příkaz CLUSRCVR , pak příkaz CLUSSDR . Pokud tak učiníte, vytvoří neověřené kanály se stavem ZASTAVENO . Poté je třeba zadat příkaz START CHANNEL , který obnoví zastavené kanály; 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. Zastavte kanály klastru.

   V systému CHICAGO zastavte kanály klastru pomocí následujících příkazů:

   ```
   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 poté odeberte všechny definice pro kanály klastru a fronty klastru z jednotlivých správců front.
8. Volitelné: Vymažte informace o klastru uložené v mezipaměti, které jsou uloženy ve správci front.

   Ačkoli tito správci front již nejsou členy klastru, uchovávají si každou kopii informací o klastru uloženou v mezipaměti. Chcete-li tato data odebrat, prohlédněte si úlohu “Obnovení správce front do stavu před klastrem” na stránce 357.

9. Nahraďte definice vzdálené fronty pro INVENTQ

   Aby síť mohla i nadále fungovat, nahraďte definici vzdálené fronty pro INVENTQ v každém správci front.

10. Uklidit clusteru.

    Odstraňte všechny definice front nebo kanálů, které již nejsou vyžadovány.

Související úlohy

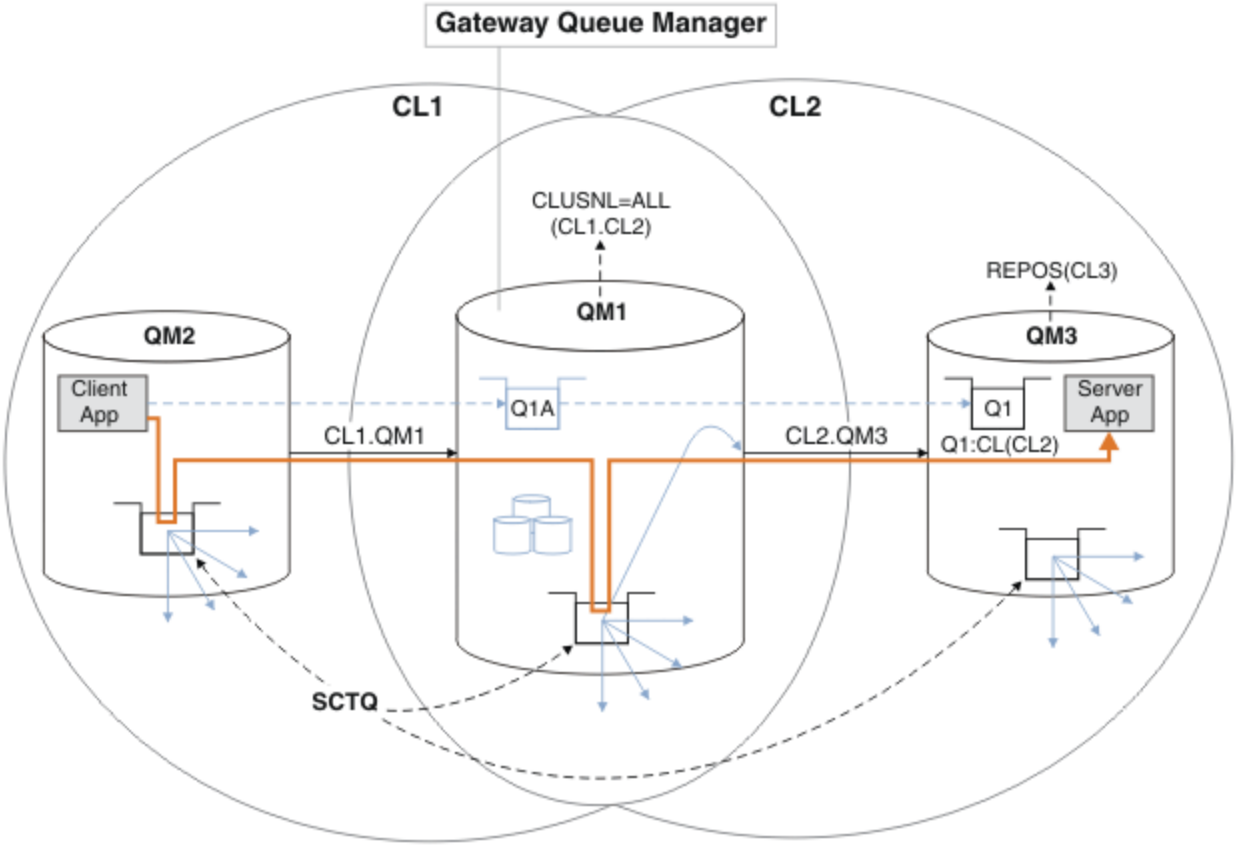
Přidání nového, vzájemně propojeného klastru
Přidejte nový klastr, který sdílí některé správce front s existujícím klastrem.

Vytvoření dvou překrývajících se klastrů se správcem front brány

Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv 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 47 na stránce 331. Příklad je popsán v tématu Klastrování: Izolace aplikace pomocí více přenosových front klastru.



Obrázek 47. Aplikace klient-server implementovaná na centrální a paprskovou architekturu pomocí klastrů IBM 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 naleznete v tématu Klastrování: Plánování konfigurace přenosových front klastru.

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 QM n
strmqm QmgrName
```

Poznámka: QM4 a QM5 jsou záložní úplná úložiště pro klastry.

2. Definujte a spusťte moduly listener pro každého ze správců front.

```
*... On QM n
DEFINE LISTENER(TCP141 n) TRPTYPE(TCP) IPADDR(hostname) PORT(141 n) CONTROL(QMGR) REPLACE
START LISTENER(TCP141 n)
```

3. Vytvořte seznam názvů klastrů pro všechny klastry.

```
*... On QM1
DEFINE NAMELIST(ALL) NAMES(CL1, CL2) REPLACE
```

4. 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 332 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 QM m
DEFINE CHANNEL(CL c.QM n) CHLTYPE(CLUSSDR) CONNAME('localhost(141 n)') CLUSTER(CL c) REPLACE
DEFINE CHANNEL(CL c.QM m) CHLTYPE(CLUSRCVR) CONNAME('localhost(141 m)') CLUSTER(CL c) REPLACE
```

6. Přidejte správce front brány 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.

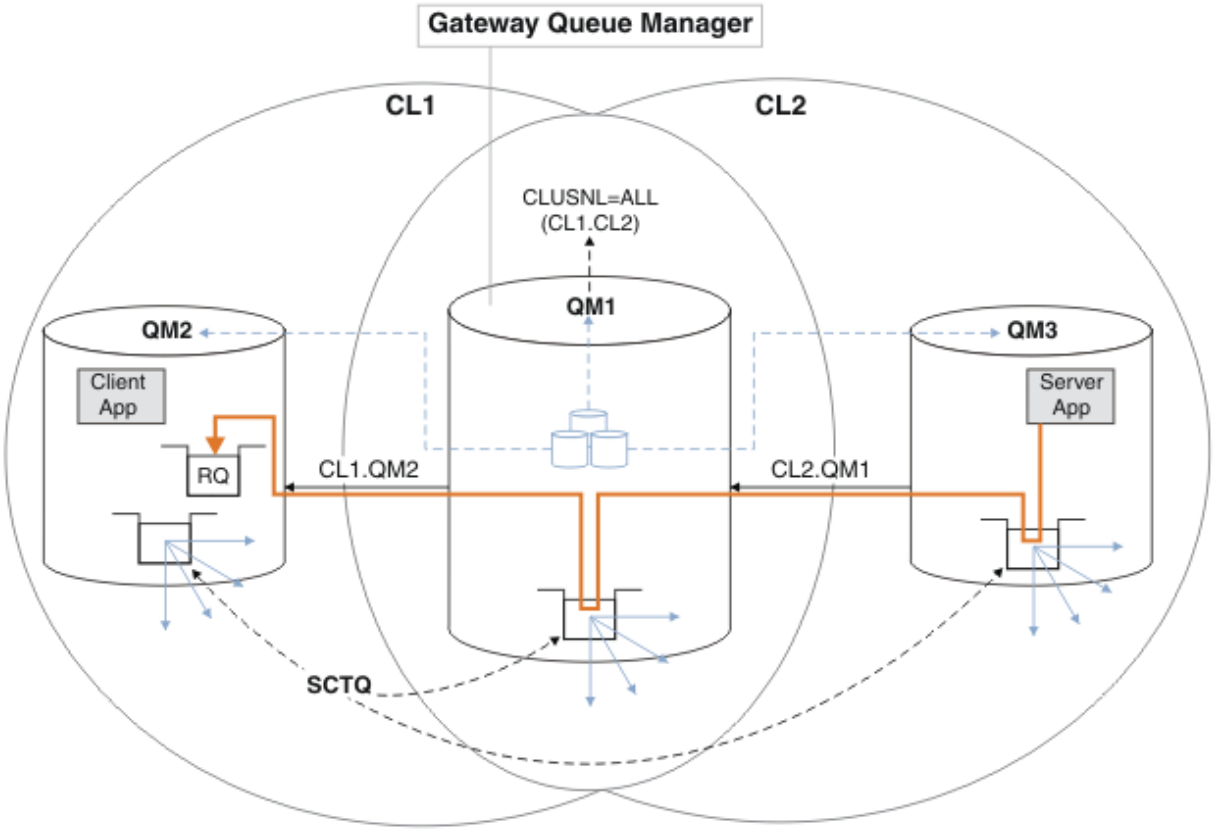
```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

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 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.

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: IBM 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

Klastrování: Izolace aplikace pomocí více přenosových front klastru

Související úlohy

Klastrování: Plánování konfigurace přenosových front klastru

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 310

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a samostatný odesílací kanál a přenosovou frontu.

Než začnete

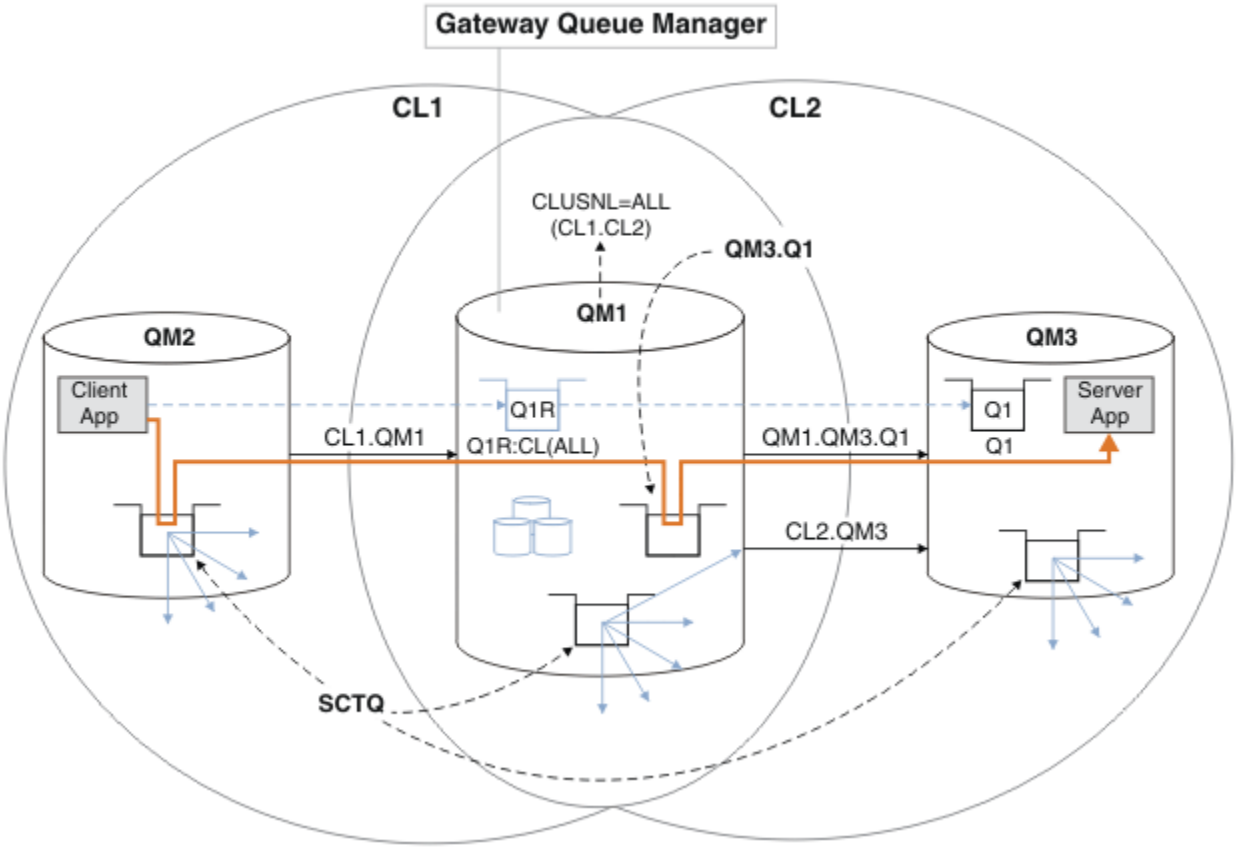
Vytvořte překrývající se klastry zobrazené v aplikaci Client-server implementované na centrální a paprskovou architekturu pomocí IBM MQ klastrů v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 331 podle kroků v této úloze.

Informace o této úloze

Řešení používá distribuované řazení do front k oddělení zpráv pro aplikaci `Server App` od ostatních přenosů zpráv ve správci front brány. Chcete-li přesměrovat zprávy na jinou přenosovou frontu a jiný kanál, musíte v systému `QM1` definovat definici klastrované vzdálené fronty. Definice vzdálené fronty musí obsahovat odkaz na specifickou přenosovou frontu, která ukládá zprávy pouze pro `Q1` on `QM3`. V produktu Obrázek 49 na stránce 336je alias fronty klastru `Q1A` doplněn o definici vzdálené fronty `Q1R`a přidána přenosová fronta a kanál odesilatele.

V tomto řešení jsou všechny zprávy odpovědi vráceny pomocí obecného `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Výhodou tohoto řešení je, že je snadné oddělit provoz pro více cílových front ve stejném správci front ve stejném klastru. Nevýhodou řešení je, 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 pro izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 338. Musíte také spravovat přepínač z jedné přenosové fronty do druhé.



Obrázek 49. Aplikace typu klient-server implementovaná do centrálního a paprskového klastru s použitím definic vzdálených front.

Postup

1. Vytvořte kanál pro oddělení provozu zpráv pro produkt `Q1` od správce front brány.
   a) Vytvořte odesílací kanál ve správci front brány `QM1`pro cílového správce front `QM3`.

```
DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(SDR) CONNAME(QM3HostName(1413)) XMITQ(QM3.Q1) REPLACE
```

b) Vytvořte přijímací kanál v cílovém správci front QM3.

```
DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(RCVR) REPLACE
```

2. Vytvořit přenosovou frontu ve správci front brány pro přenos zpráv do produktu Q1

```
DEFINE QLOCAL(QM3.Q1) USAGE(XMITQ) REPLACE
START CHANNEL(QM1.QM3.Q1)
```

Spuštění kanálu, který je přidružen k přenosové frontě, přidruží přenosovou frontu ke kanálu. Kanál se spustí automaticky, jakmile je přenosová fronta přidružena ke kanálu.

3. Doplňte definici aliasu klastrované fronty pro Q1 ve správci front brány o definici klastrované vzdálené fronty.

```
DEFINE QREMOTE CLUSNL(ALL) RNAME(Q1) RQMNAME(QM3) XMITQ(QM3.Q1) REPLACE
```

Jak pokračovat dále

Otestujte konfiguraci odesláním zprávy do systému Q1 on QM3 z QM2 pomocí vzdálené definice klastrované fronty Q1R ve správci front brány QM1.

1. Spusťte ukázkový program **amqsput** na QM2 , abyste vložili 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. 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 Q1R>
no more messages
Sample AMQSGET0 end
```

Související pojmy

Klastrování: Izolace aplikace pomocí více přenosových front klastru

Řízení přístupu a více přenosových front klastru

Související úlohy

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další přenosovou frontu klastru k oddělení přenosu zpráv do jednoho správce front v klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další klastr k izolaci zpráv do konkrétní fronty klastru.

Změna výchozího nastavení na oddělení přenosových front klastru pro izolaci přenosu zpráv
Můžete změnit výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě. Změna výchozího nastavení vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

Klastrování: Plánování konfigurace přenosových front klastru
“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 310
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další přenosovou frontu klastru k oddělení přenosu zpráv do jednoho správce front v klastru.

Než začnete

1. Správce front brány musí být na systému IBM MQ.
2. Vytvořte překrývající se klastry zobrazené v aplikaci Client-server implementované na centrální a paprskovou architekturu pomocí IBM MQ klastrů v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 331 podle kroků v této úloze.

Informace o této úloze

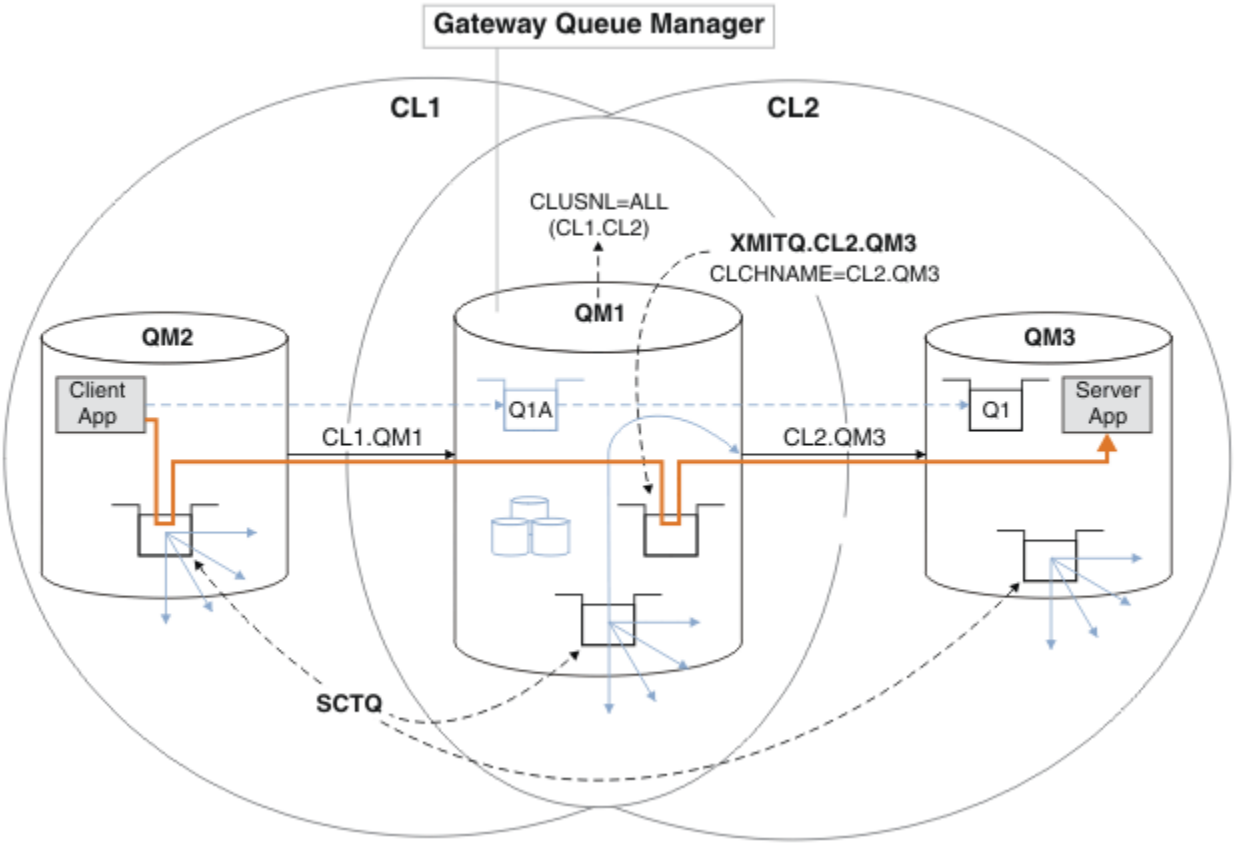
Ve správci front brány `QM1`přidejte přenosovou frontu a nastavte její atribut fronty `CLCHNAME`. Nastavte `CLCHNAME` na název přijímacího kanálu klastru na `QM3` ; viz Obrázek 50 na stránce 339.

Toto řešení má řadu výhod oproti řešení popsanému v části “Přidání definice vzdálené fronty pro izolování zpráv odeslaných ze správce front brány” na stránce 335:

- Vyžaduje méně dalších definic.
- Podporuje vyrovnávání 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 při restartování kanálu bez ztráty zpráv.
- Správce front brány pokračuje v předávání zpráv ve stejném pořadí, v jakém je obdržel. Činí tak i v případě, že dojde k přepnutí se zprávami pro frontu `Q1` ve `QM3` stále zapnuté `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Konfigurace pro izolování provozu zpráv klastru v produktu Obrázek 50 na stránce 339 nevede k tak velké izolaci provozu jako konfigurace používající vzdálené fronty v produktu “Přidání definice vzdálené fronty pro izolování zpráv odeslaných ze správce front brány” na stránce 335. Pokud je správce front `QM3` v produktu `CL2` hostitelem řady různých front klastru a serverových aplikací, všechny tyto fronty sdílejí kanál klastru `CL2.QM3`a připojují se `QM1` k `QM3`. Další toky jsou znázorněny v souboru Obrázek 50 na stránce 339 šedou šipkou představující potenciální přenos zpráv klastru z `SYSTEM.CLUSTER.TRANSMIT.QUEUE` do odesílacího kanálu klastru `CL2.QM3`.

Řešením je omezit správce front na hostování jedné fronty klastru v konkrétním klastru. Pokud je správce front již hostitelem řady front klastru, musíte pro splnění tohoto omezení buď vytvořit jiného správce front, nebo vytvořit jiný klastr; viz “Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaných ze správce front brány” na stránce 341.



Obrázek 50. Aplikace typu klient-server byla implementována na centrální a paprskovou architekturu pomocí 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 přenosovou frontu `XMITQ.CL2.QM3`.
   a) Zastavte odesílací kanál klastru `CL2.QM3`.

```
*... On QM1
STOP CHANNEL(CL2.QM3)
```

   Odpověď je, že příkaz je přijat:

```
AMQ8019: Stop IBM MQ channel accepted.
```

   b) Zkontrolujte, zda je kanál `CL2.QM3` zastaven.

   Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou FORCE . Příkladem nastavení volby FORCE může být, pokud se kanál nezastaví a vy nemůžete restartovat druhého správce front, aby synchronizoval kanál.

```
*... 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, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

d) Zkontrolujte, zda byl 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 přepnuta.

Monitorujte protokol chyb správce front brány pro zprávu " AMQ7341 `Fronta přenosu pro kanál CL2.QM3 má hodnotu XMITQ.CL2.QM3` ".

Jak pokračovat dále

Otestujte oddělenou přenosovou frontu odesláním zprávy z `QM2` do `Q1` na `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

Klastrování: Izolace aplikace pomocí více přenosových front klastru

"Práce s přenosovými frontami klastru a odesílacími kanály klastru" na stránce 289
Zprávy mezi klastrovanými správci front jsou uloženy v přenosových frontách klastru a předávány odesílacími kanály klastru. V libovolném časovém okamžiku je odesílací kanál klastru přidružen k jedné přenosové frontě. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizované a transakční.

Související úlohy

Přidání definice vzdálené fronty pro izolování zpráv odeslaných ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a samostatný odesílací kanál a přenosovou frontu.

Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaných ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další klastr k izolaci zpráv do konkrétní fronty klastru.

Změna výchozího nastavení na oddělení přenosových front klastru pro izolaci přenosu zpráv
Můžete změnit výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě. Změna výchozího nastavení vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

Klastrování: Plánování konfigurace přenosových front klastru

"Přidání správce front do klastru: samostatné přenosové fronty" na stránce 310
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další klastr k izolaci zpráv do konkrétní fronty klastru.

Než začnete

Kroky v úloze jsou napsány pro úpravu konfigurace znázorněné v části Obrázek 50 na stránce 339.

1. Správce front brány musí být na systému IBM MQ.
2. Vytvořte překrývající se klastry zobrazené v aplikaci Client-server implementované na centrální a paprskovou architekturu pomocí IBM MQ klastrů v produktu "Vytvoření dvou překrývajících se klastrů se správcem front brány" na stránce 331 podle kroků v této úloze.
3. Chcete-li vytvořit řešení bez dalšího klastru, postupujte podle pokynů v části Obrázek 50 na stránce 339 v části "Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 338 . Použijte jej jako základ pro kroky v této úloze.

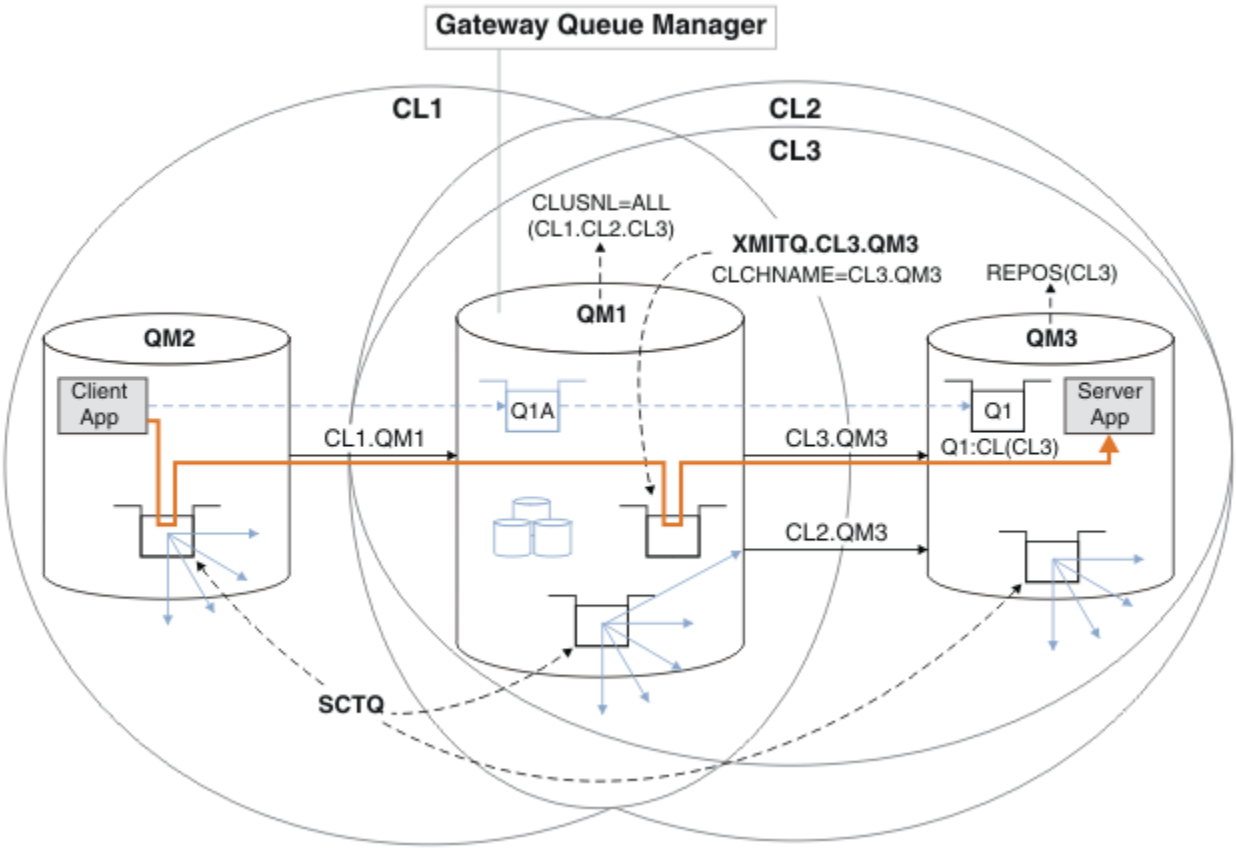
Informace o této úloze

Řešení izolace přenosu zpráv do jedné aplikace v produktu "Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 338 funguje, pokud je cílová fronta klastru jedinou frontou klastru ve správci front. Pokud tomu tak není, máte dvě možnosti. Buď přesuňte frontu do jiného správce front, nebo vytvořte klastr, který danou frontu izoluje od ostatních front klastru ve správci front.

Tato úloha vás provede kroky pro přidání klastru, abyste izolovali cílovou frontu. Klastr je přidán právě pro tento účel. V praxi přistupujte k úloze systematické izolace určitých aplikací, když jste v procesu navrhování klastrů a schémat pojmenování klastrů. Přidání klastru pokaždé, když fronta vyžaduje izolaci, může skončit s mnoha klastry, které je třeba spravovat. V této úloze změníte konfiguraci v systému “Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 338 přidáním klastru CL3 k izolaci Q1 na systému QM3. Aplikace pokračují v běhu po celou dobu změny.

Nové a změněné definice jsou zvýrazněny v souboru Obrázek 51 na stránce 342. Souhrn změn je následující: Vytvořte klastr, což znamená, že musíte také vytvořit nové úplné úložiště klastru. V příkladu je QM3 jedním z úplných úložišť pro CL3. Vytvořte odesílací a přijímací kanály klastru pro produkt QM1 pro přidání správce front brány do nového klastru. Změňte definici Q1 , abyste ji přepnuli na CL3. Upravte seznam názvů klastrů ve správci front brány a přidejte přenosovou frontu klastru, aby používala nový kanál klastru. Nakonec přepněte alias fronty Q1A na nový seznam názvů klastru.

Produkt IBM MQ nemůže automaticky přenášet zprávy z přenosové fronty XMITQ.CL2.QM3 , kterou jste přidali v produktu “Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 338 do nové přenosové fronty XMITQ.CL3.QM3. Může automaticky přenášet zprávy pouze v případě, že jsou obě přenosové fronty obsluhovány stejným kanálem odesilatele klastru. Místo toho úloha popisuje jeden způsob, jak provést přepínač ručně, což může být pro vás vhodné. Po dokončení přenosu máte možnost vrátit se k použití výchozí přenosové fronty klastru pro ostatní CL2 fronty klastru v systému QM3. Nebo můžete pokračovat v používání XMITQ.CL2.QM3. Pokud se rozhodnete přejít zpět na výchozí přenosovou frontu klastru, správce front brány bude automaticky spravovat přepínač.



Obrázek 51. Použití dalšího klastru k oddělení provozu zpráv ve správci front brány, který přechází do jedné z několika front klastru ve stejném správci front.

Postup

1. Změňte správce front QM3 a QM5 tak, aby z nich byla úložiště pro CL2 i CL3.

Aby se správce front stal členem více klastrů, musí použít seznam názvů klastrů k identifikaci klastrů, jejichž je členem.

```
*... 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 pro 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 adresáře CL3.

   Přidejte správce front brány přidáním QM1 do CL3 jako částečného úložiště. Vytvořte dílčí úložiště přidáním kanálů odesilatele klastru a příjemce klastru do souboru 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 QM1pro zprávy, které budou v systému CL3 on QM3.

   Na začátku zastavte odesílací kanál klastru přenášející zprávy z přenosové fronty, dokud nebudete připraveni přepínat přenosové fronty.

```
*... On QM1
DEFINE QLOCAL(XMITQ.CL3.QM3) USAGE(XMITQ) CLCHNAME(CL3.QM3) GET(DISABLED) REPLACE
```

5. Vyprázdnit zprávy z existující přenosové fronty klastru XMITQ.CL2.QM3.

   Cílem této dílčí procedury je zachovat pořadí zpráv v produktu Q1 tak, aby odpovídalo pořadí, v jakém dorazily do správce front brány. U klastrů není řazení zpráv plně zaručeno, ale je pravděpodobné. Je-li vyžadováno zaručené řazení zpráv, aplikace musí definovat pořadí zpráv; viz Pořadí, ve kterém jsou zprávy načítány z fronty.

   a) Změňte cílovou frontu Q1 na QM3 z CL2 na CL3.

```
*... On QM3
ALTER QLOCAL(Q1) CLUSTER(CL3)
```

   b) Monitorujte produkt XMITQ.CL3.QM3 , dokud do něj nezačnou být doručovány zprávy.

      Zprávy se začínají doručovat do produktu XMITQ.CL3.QM3 , když se přepínač Q1 na CL3 rozšíří do správce front brány.

```
*... On QM1
DISPLAY QUEUE(XMITQ.CL3.QM3) CURDEPTH
```

   c) Monitorujte systém XMITQ.CL2.QM3 , dokud nebude mít žádné zprávy čekající na doručení do systému Q1 on QM3.

      Poznámka: Produkt XMITQ.CL2.QM3 může ukládat zprávy pro jiné fronty v systému QM3 , které jsou členy produktu CL2. V takovém případě nemusí hloubka 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. Odeberte starou přenosovou frontu klastru XMITQ.CL2.QM3, pokud již není požadována.

   Zprávy pro fronty klastru v systému CL2 on 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 z nich závisí na tom, zda je hodnota atributu správce front **DEFCLXQ** v systému QM1 SCTQ nebo CHANNEL. Správce front přenáší zprávy z produktu XMITQ.CL2.QM3 automaticky při příštím spuštění odesílacího kanálu klastru CL2.QM3 .

   a) Změňte přenosovou frontu XMITQ.CL2.QM3z přenosové fronty klastru na normální přenosovou frontu.

      Tím se přeruší přidružení přenosové fronty k libovolným odesílacím kanálům klastru. V odezvě produkt IBM MQ automaticky přenese zprávy z produktu XMITQ.CL2.QM3 do výchozí přenosové fronty klastru při příštím spuštění odesílacího kanálu klastru. Do té doby budou zprávy pro CL2 on QM3 i nadále umístěny na XMITQ.CL2.QM3.

      ```
      *... On QM1
      ALTER QLOCAL(XMITQ.CL2.QM3) CLCHNAME(' ')
      ```

   b) Zastavte odesílací kanál klastru CL2.QM3.

      Zastavení a restartování odesílacího kanálu klastru zahájí přenos zpráv z produktu XMITQ.CL2.QM3 do výchozí přenosové fronty klastru. Obvykle byste zastavili a spustili kanál ručně, abyste spustili přenos. Přenos se spustí automaticky, pokud se kanál restartuje po ukončení po uplynutí intervalu odpojení.

      ```
      *... On QM1
      STOP CHANNEL(CL2.QM3)
      ```

      Odpověď je, že příkaz je přijat:

      ```
      AMQ8019: Stop IBM MQ channel accepted.
      ```

   c) Zkontrolujte, zda je kanál CL2.QM3 zastaven.

      Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou FORCE . Příkladem nastavení volby FORCE může být, pokud se kanál nezastaví a vy nemůžete restartovat druhého správce front, aby synchronizoval kanál.

      ```
      *... 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, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

e) Zkontrolujte, zda byl 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) Monitorujte protokol chyb správce front brány pro zprávu " AMQ7341 Fronta přenosu pro kanál CL2.QM3 má hodnotu 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 samostatně klastrovanou frontu odesláním zprávy z QM2 do Q1 na 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

Klastrování: Izolace aplikace pomocí více přenosových front klastru

“Práce s přenosovými frontami klastru a odesílacími kanály klastru” na stránce 289

Zprávy mezi klastrovanými správci front jsou uloženy v přenosových frontách klastru a předávány odesílacími kanály klastru. V libovolném časovém okamžiku je odesílací kanál klastru přidružen k jedné přenosové frontě. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizované a transakční.

Související úlohy

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a samostatný odesílací kanál a přenosovou frontu.

Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další přenosovou frontu klastru k oddělení přenosu zpráv do jednoho správce front v klastru.

Změna výchozího nastavení na oddělení přenosových front klastru pro izolaci přenosu zpráv
Můžete změnit výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě. Změna výchozího nastavení vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

Klastrování: Plánování konfigurace přenosových front klastru

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 310
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Můžete změnit výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě. Změna výchozího nastavení vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

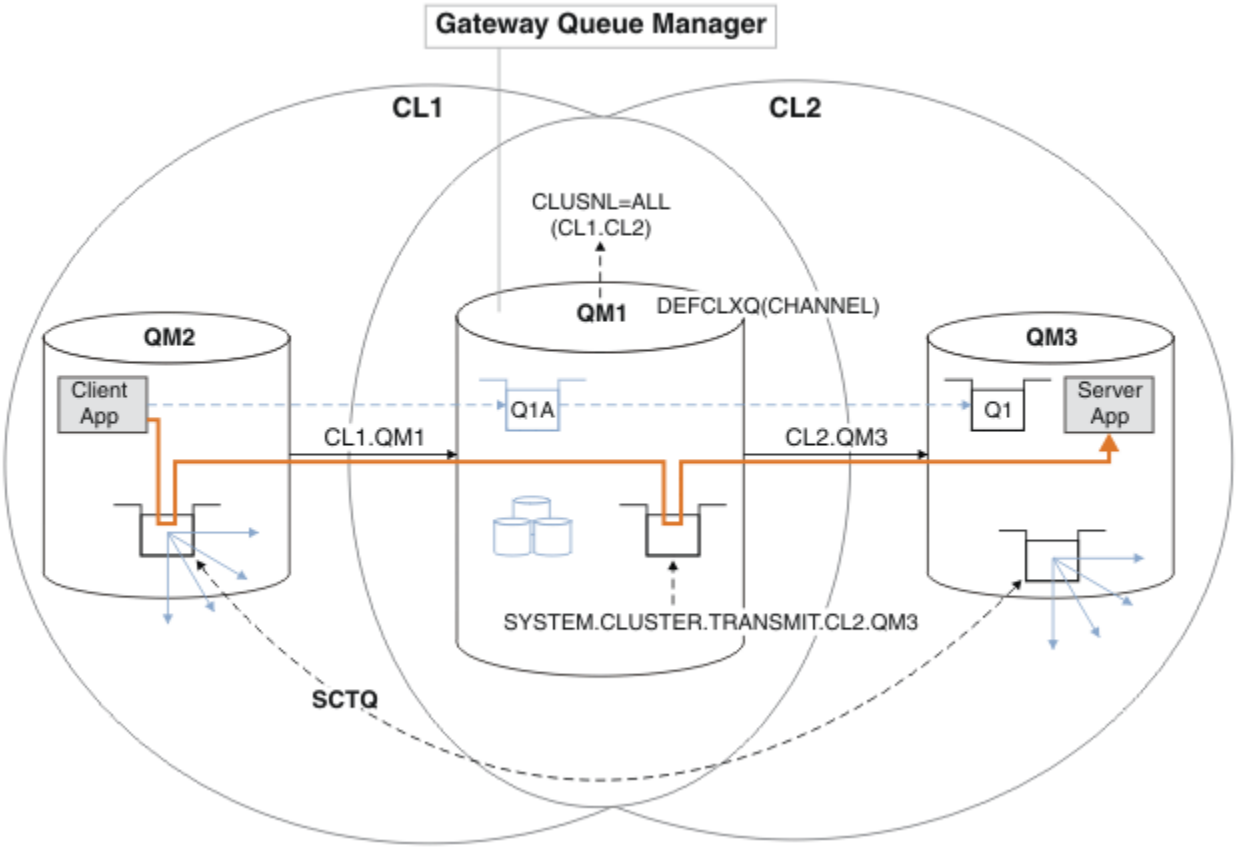
Než začnete

1. Správce front brány musí být na systému IBM MQ.
2. Vytvořte překrývající se klastry zobrazené v aplikaci Client-server implementované na centrální a paprskovou architekturu pomocí IBM MQ klastrů v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 331 podle kroků v této úloze.

Informace o této úloze

Chcete-li implementovat architekturu s více frontami klastrů, musí být váš správce front brány v systému IBM MQ. Při použití více přenosových front klastru je nutné změnit výchozí typ přenosové fronty klastru ve správci front brány. Změňte hodnotu atributu správce front **DEFCLXQ** v systému `QM1` z `SCTQ` na `CHANNEL` ; viz Obrázek 52 na stránce 347. Diagram zobrazuje jeden tok zpráv. Pro toky do jiných správců front nebo do jiných klastrů vytvoří správce front další trvalé přenosové fronty dynamického klastru. Každý odesílací kanál klastru přenáší zprávy z jiné přenosové fronty klastru.

Změna se neprojeví okamžitě, pokud poprvé nepřipojujete správce front brány ke klastrům. Úloha zahrnuje kroky pro typický případ správy změny existující konfigurace. Chcete-li nastavit správce front tak, aby při prvním připojení ke klastru používal samostatné přenosové fronty klastru, viz “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 310.



Obrázek 52. Aplikace typu klient-server byla implementována do centrálního serveru a hovořila s architekturou se samostatnými přenosovými frontami klastru ve správci front brány.

Postup

1. Změňte správce front brány tak, aby používal samostatné přenosové fronty klastru.

```
*... On QM1
ALTER QMGR DEFCLXQ(CHANNEL)
```

2. Přepněte do samostatných přenosových front klastru.

   Jakýkoli odesílací kanál klastru, který neběží, se při příštím spuštění přepne na použití samostatných přenosových front klastru.

   Chcete-li přepnout spuštěné kanály, buď restartujte 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 zpráv o 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, že příkaz je přijat:

```
AMQ8019: Stop IBM MQ channel accepted.
```

c) Monitorovat, které kanály jsou zastaveny

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
```

Odezva je seznam kanálů, které jsou stále spuštěny, a kanálů, 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 spustit příkaz **STOP CHANNEL** znovu s volbou FORCE . Příkladem nastavení volby FORCE může být, pokud se kanál nezastaví a vy nemůžete restartovat druhého správce front, aby synchronizoval kanál.

```
*... On QM1
START CHANNEL(CL2.QM5)
```

Odpověď je, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

e) Monitorujte přepínané přenosové fronty.

Monitorujte protokol chyb správce front brány pro zprávu " AMQ7341 Fronta přenosu pro kanál CL2.QM3 má hodnotu SYSTEM.CLUSTER.TRANSMIT. *QUEUE*|*CL2.QM3* ".

f) Zkontrolujte, zda se soubor SYSTEM.CLUSTER.TRANSMIT.QUEUE již nepoužívá.

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
DISPLAY QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE) CURDEPTH
```

Odezva je seznam zpráv o stavu kanálu a hloubka SYSTEM.CLUSTER.TRANSMIT.QUEUE:

```
AMQ8420: Channel Status not found.
AMQ8409: Display Queue details.
QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE)    TYPE(QLOCAL)
CURDEPTH(0)
```

g) Monitorování, které kanály jsou spuštěny

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
```

Odezva je seznam kanálů, v tomto případě již spuštěných 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. Otestujte automaticky definovanou přenosovou frontu klastru odesláním zprávy z QM2 do Q1 v systému QM3a vyřešte název fronty 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. Zvažte, zda znovu nakonfigurovat zabezpečení, a to konfigurací zabezpečení pro fronty klastru ve správcích front, ze kterých pocházejí zprávy pro fronty klastru.

Související pojmy

Řízení přístupu a více přenosových front klastru

Klastrování: Izolace aplikace pomocí více přenosových front klastru

Související úlohy

Přidání definice vzdálené fronty pro izolování zpráv odeslaných ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a samostatný odesílací kanál a přenosovou frontu.

Přidání přenosové fronty klastru pro izolování přenosu zpráv klastru odeslaného ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další přenosovou frontu klastru k oddělení přenosu zpráv do jednoho správce front v klastru.

Přidání klastru a přenosové fronty klastru pro izolování provozu zpráv klastru odeslaných ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenosu zpráv o úpravách do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako jiné zprávy klastru. Řešení používá další klastr k izolaci zpráv do konkrétní fronty klastru.

Klastrování: Plánování konfigurace přenosových front klastru

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 310
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů. Zprávy do front klastru a témata se přenášejí pomocí více přenosových front klastru.

Odebrání fronty klastru ze správce front

Zakažte frontu INVENTQ v Torontu. Odešlete všechny zprávy inventáře do New Yorku a odstraňte frontu INVENTQ v Torontu, když je prázdná.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Přidání správce front, který je hostitelem fronty” na stránce 315. Obsahuje čtyři správce front. LONDON a NEWYORK obě obsahují úplná úložiště. PARIS a TORONTO zadržují dílčí úložiště. Aplikace inventáře je spuštěna na systémech v New Yorku a Torontu a je řízena příchodem zpráv do fronty INVENTQ .
- Kvůli snížené pracovní zátěži již nechcete spouštět aplikaci inventáře v Torontu. Chcete zakázat frontu INVENTQ , jejímž hostitelem je správce front TORONTO, a nechat TORONTO zprávy kanálu do fronty INVENTQ v NEWYORK.
- 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. Změňte parametr INVENTQ na systému TORONTO tak, aby nebyl přístupný ze zbytku klastru:

   ```
   ALTER QLOCAL(INVENTQ) CLUSTER(' ')
   ```

2. Zkontrolujte, zda fronta již není k dispozici.

   Ve správci front úplného úložiště LONDON nebo NEWYORKzkontrolujte, zda fronta již není hostitelem správce front TORONTO , zadáním následujícího příkazu:

   ```
   DIS QCLUSTER (INVENTQ)
   ```

   Parametr TORONTO není uveden ve výsledcích, pokud byl příkaz ALTER úspěšně dokončen.

3. Zakažte frontu.

   Zakažte frontu INVENTQ v adresáři TORONTO , aby do ní nebylo možné zapisovat žádné další zprávy:

   ```
   ALTER QLOCAL(INVENTQ) PUT(DISABLED)
   ```

   Nyní zprávy přenášené do této fronty pomocí příkazu MQOO_BIND_ON_OPEN přejdou do fronty nedoručených zpráv. Je třeba zabránit všem aplikacím v explicitním vkládání zpráv do fronty v tomto správci front.

4. Monitorujte frontu, dokud nebude prázdná.

   Monitorujte frontu pomocí příkazu DISPLAY QUEUE , uveďte atributy IPPROCS, OPPROCSa CURDEPTH, nebo použijte příkaz **WRKMQMSTS** na systému IBM i. Je-li počet vstupních a výstupních procesů a aktuální hloubka front nulová, fronta je prázdná.

5. Monitorujte kanál, abyste se ujistili, že neexistují žádné neověřené zprávy.

   Chcete-li se ujistit, že v kanálu INVENTORY.TORONTOnejsou žádné zprávy s pochybnostmi, monitorujte kanál odesilatele klastru nazvaný INVENTORY.TORONTO na všech ostatních správcích front. Zadejte příkaz DISPLAY CHSTATUS s parametrem INDOUBT pro každého správce front:

   ```
   DISPLAY CHSTATUS(INVENTORY.TORONTO) INDOUBT
   ```

Pokud existují nějaké zprávy s pochybnostmi, musíte je před pokračováním vyřešit. Můžete se například pokusit o zadání příkazu RESOLVE channel nebo o zastavení a restartování kanálu.

6. Odstraňte lokální frontu.

   Když jste spokojeni s tím, že neexistují žádné další zprávy, které by mohly být doručeny do aplikace inventáře na adrese TORONTO, můžete frontu odstranit:

   ```
   DELETE QLOCAL(INVENTQ)
   ```

7. Nyní můžete odebrat aplikaci inventáře ze systému v Torontu

   Odebráním aplikace se vyhnete duplikaci a ušetříte místo v systému.

Výsledky

Klastr nastavený touto úlohou je podobný klastru nastaveným předchozí úlohou. Rozdíl je v tom, že fronta INVENTQ již není ve správci front k dispozici TORONTO.

Když jste v kroku 1 vyjali frontu z provozu, správce front TORONTO odeslal zprávu dvěma správcům front úplného úložiště. Upozornil je na změnu stavu. Správci front úplného úložiště předávají tyto informace ostatním správcům front v klastru, kteří požadovali aktualizace informací týkajících se produktu INVENTQ.

Když správce front vloží zprávu do fronty INVENTQ , aktualizované dílčí úložiště označuje, že fronta INVENTQ je k dispozici pouze ve správci front NEWYORK . Zpráva je odeslána správci front NEWYORK .

Jak pokračovat dále

V této úloze byla pouze jedna fronta, kterou bylo možné odebrat, a pouze jeden klastr, ze kterého bylo možné odebrat.

Předpokládejme, že existuje mnoho front odkazujících na seznam názvů obsahující mnoho názvů klastrů. Například správce front TORONTO může hostovat nejen INVENTQ, ale také PAYROLLQ, SALESQa PURCHASESQ. Produkt TORONTO zpřístupní tyto fronty ve všech příslušných klastrech, INVENTORY, PAYROLL, SALESa PURCHASES. Definujte seznam názvů klastrů ve správci front 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 TOROLIST tak, aby z něj byl odebrán název klastru SALES .

Chcete-li odebrat jednu frontu z jednoho z klastrů v seznamu názvů, vytvořte seznam názvů obsahující zbývající seznam názvů klastrů. Poté změňte definici fronty tak, aby používala nový seznam názvů. Chcete-li odebrat soubor 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 PAYROLLQ :

```
ALTER QLOCAL(PAYROLLQ) CLUSNL(TOROSHORTLIST)
```

Odebrání správce front z klastru: doporučený postup

Odeberte správce front z klastru ve scénářích, kde může správce front normálně komunikovat s alespoň jedním úplným úložištěm v klastru.

Než začnete

Tato metoda je doporučeným postupem pro scénáře, ve kterých je k dispozici alespoň jedno úplné úložiště, a může být kontaktována odebíraným správcem front. Tato metoda zahrnuje nejmenší ruční zásah a umožňuje správci front vyjednat řízené stažení z klastru. Pokud odebíraný správce front nemůže kontaktovat úplné úložiště, postupujte podle části “Odebrání správce front z klastru: alternativní metoda” na stránce 355.

Informace o této úloze

Tato ukázková úloha odebere správce front LONDON z klastru INVENTORY . Klastr INVENTORY je nastaven podle popisu v části “Přidání správce front do klastru” na stránce 308a upraven podle popisu v části “Odebrání fronty klastru ze správce front” na stránce 350.

Proces odebrání správce front z klastru je složitější než 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. V připojovaném správci front musí být vytvořeny nové odesílací a přijímací kanály, aby se mohl připojit k úplnému úložišti.

Pokud je správce front odebrán z klastru, je pravděpodobné, že aplikace připojené ke správci front používají objekty, jako jsou fronty, jejichž hostitelem je jiné místo v klastru. Také aplikace, které jsou připojeny k jiným správcům front v klastru, mohou používat objekty, jejichž hostitelem je cílový správce 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 používal pro připojení ke klastru. Každý správce front v klastru má kopii dat uložených v mezipaměti, která popisuje ostatní členy klastru. To může zahrnovat ten, který se odebírá.

Postup

1. Před odebráním správce front z klastru se ujistěte, že již není hostitelem prostředků, které klastr potřebuje:
   - Pokud je správce front hostitelem úplného úložiště, proveďte kroky 1-6 z adresáře “Přesunutí úplného úložiště do jiného správce front” na stránce 320. Pokud funkce úplného úložiště správce front, který má být odebrán, nemá být přesunuta do jiného správce front, je nutné provést pouze kroky 5 a 6.
   - Pokud je správce front hostitelem front klastru, proveďte kroky 1-7 z adresáře “Odebrání fronty klastru ze správce front” na stránce 350.
   - Pokud je správce front hostitelem témat klastru, buď odstraňte témata (například pomocí příkazu DELETE TOPIC), nebo je přesuňte do jiných hostitelů, jak je popsáno v tématu “Přesunutí definice tématu klastru do jiného správce front” na stránce 428.

     Poznámka: Pokud odeberete správce front z klastru a správce front bude i nadále hostitelem tématu klastru, může se správce front i nadále pokoušet doručovat publikace správcům front, kteří jsou v klastru ponecháni, dokud nebude téma odstraněno.
2. Upravte ručně definované přijímací kanály klastru tak, aby byly odebrány z klastru ve správci front LONDON:

```
ALTER CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) CLUSTER(' ')
```

3. Upravte ručně definované odesílací kanály klastru tak, aby byly odebrány z klastru ve správci front LONDON:

```
ALTER CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSSDR) CLUSTER(' ')
```

   Ostatní správci front v klastru zjišťují, že tento správce front a jeho prostředky klastru již nejsou součástí klastru.
4. Monitorujte přenosovou frontu klastru ve správci front LONDON, dokud nebudou k dispozici žádné zprávy, které čekají na tok do jakéhokoli úplného úložiště v klastru.

```
DISPLAY CHSTATUS(INVENTORY.PARIS) XQMSGSA
```

   Pokud zprávy zůstávají v přenosové frontě, před pokračováním určete, proč nejsou odesílány do úplných úložišť PARIS a NEWYORK .

Výsledky

Správce front LONDON již není součástí klastru. Může však i nadále fungovat jako nezávislý správce front.

Jak pokračovat dále

Výsledek těchto změn lze potvrdit zadáním následujícího příkazu na zbývajících členech klastru:

```
DISPLAY CLUSQMGR(LONDON)
```

Správce front se bude nadále zobrazovat, dokud se automaticky definované odesílací kanály klastru nezastaví. Můžete počkat, až k tomu dojde, nebo pokračovat v monitorování aktivních instancí zadáním následujícího příkazu:

```
DISPLAY CHANNEL(INVENTORY.LONDON)
```

Jste-li si jisti, že do tohoto správce front nejsou doručovány žádné další zprávy, můžete kanály odesilatele klastru do produktu LONDON zastavit zadáním následujícího příkazu pro zbývající členy klastru:

```
STOP CHANNEL(INVENTORY.LONDON) STATUS(INACTIVE)
```

Po rozšíření změn v rámci klastru a po nedoručení dalších zpráv do tohoto správce front zastavte a odstraňte kanál CLUSRCVR v systému LONDON:

```
STOP CHANNEL(INVENTORY.LONDON)
DELETE CHANNEL(INVENTORY.LONDON)
```

Pokud byla pro tento kanál používána ručně definovaná přenosová fronta a vzor CLCHNAME neodpovídá žádnému jinému existujícímu nebo plánovanému kanálu, možná budete chtít přenosovou frontu odstranit. Příklad:

```
DELETE QLOCAL(PARIS.CUSTOM.XMITQ)
```

Poznámka: V případě automaticky definovaných přenosových front nebo sdíleného SYSTEM.CLUSTER.TRANSMIT.QUEUE se používá, tento krok není povinný.

Odebraného správce front lze později přidat zpět do klastru, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 308. Odebraný správce front bude nadále ukládat do mezipaměti informace o zbývajících členech klastru po dobu až 90 dnů. Pokud nechcete čekat na vypršení platnosti této mezipaměti, můžete ji vynuceně odebrat, jak je popsáno v tématu “Obnovení správce front do stavu před klastrem” na stránce 357.

Související úlohy

Odebrání správce front z klastru (pomocí IBM MQ Explorer)

Související odkazy

ALTER CHANNEL (změna nastavení kanálu)

DISPLAY CHANNEL (zobrazit definici kanálu)

DISPLAY CHSTATUS (zobrazení stavu kanálu)

DISPLAY CLUSQMGR (zobrazit informace o kanálu pro správce front klastru)

STOP CHANNEL (zastavení kanálu)

Odebrání správce front z klastru: alternativní metoda

Odeberte správce front z klastru ve scénářích, kde kvůli značnému problému se systémem nebo konfigurací nemůže správce front komunikovat s žádným úplným úložištěm v klastru.

Než začnete

Tato alternativní metoda ručního odebrání správce front z klastru 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, kde odebíraný správce front nemůže komunikovat s žádným z úplných úložišť. Příčinou může být například skutečnost, že správce front přestal pracovat nebo že došlo k dlouhotrvajícímu selhání komunikace mezi správcem front a klastrem. Jinak použijte nejběžnější metodu: “Odebrání správce front z klastru: doporučený postup” na stránce 353.

Informace o této úloze

Tato ukázková úloha odebere správce front `LONDON` z klastru `INVENTORY` . Klastr `INVENTORY` je nastaven podle popisu v části “Přidání správce front do klastru” na stránce 308a upraven podle popisu v části “Odebrání fronty klastru ze správce front” na stránce 350.

Proces odebrání správce front z klastru je složitější než 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. V připojovaném správci front musí být vytvořeny nové odesílací a přijímací kanály, aby se mohl připojit k úplnému úložišti.

Pokud je správce front odebrán z klastru, je pravděpodobné, že aplikace připojené ke správci front používají objekty, jako jsou fronty, jejichž hostitelem je jiné místo v klastru. Také aplikace, které jsou připojeny k jiným správcům front v klastru, mohou používat objekty, jejichž hostitelem je cílový správce 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 používal pro připojení ke klastru. Každý správce front v klastru má kopii dat uložených v mezipaměti, která popisuje ostatní členy klastru. To může zahrnovat ten, který se odebírá.

Tento postup může být vhodný v případě nouze, kdy není možné čekat na řádné opuštění klastru správcem front.

Postup

1. Před odebráním správce front z klastru se ujistěte, že již není hostitelem prostředků, které klastr potřebuje:
   - Pokud je správce front hostitelem úplného úložiště, proveďte kroky 1-6 z adresáře “Přesunutí úplného úložiště do jiného správce front” na stránce 320. Pokud funkce úplného úložiště správce

front, který má být odebrán, nemá být přesunuta do jiného správce front, je nutné provést pouze kroky 5 a 6.

- Pokud je správce front hostitelem front klastru, proveďte kroky 1-7 z adresáře "Odebrání fronty klastru ze správce front" na stránce 350.
- Pokud je správce front hostitelem témat klastru, buď odstraňte témata (například pomocí příkazu DELETE TOPIC), nebo je přesuňte do jiných hostitelů, jak je popsáno v tématu "Přesunutí definice tématu klastru do jiného správce front" na stránce 428.

  Poznámka: Pokud odeberete správce front z klastru a správce front bude i nadále hostitelem tématu klastru, může se správce front i nadále pokoušet doručovat publikace správcům front, kteří jsou v klastru ponecháni, dokud nebude téma odstraněno.

2. Zastavte všechny kanály používané ke komunikaci s ostatními správci front v klastru. Pomocí volby MODE(FORCE) zastavte kanál CLUSRCVR ve správci front LONDON. V opačném případě může být nutné počkat na zastavení kanálu odesílajícího správce front:

```
STOP CHANNEL(INVENTORY.LONDON) MODE(FORCE)
STOP CHANNEL(INVENTORY.TORONTO)
STOP CHANNEL(INVENTORY.PARIS)
STOP CHANNEL(INVENTORY.NEWYORK)
```

3. Monitorujte stavy kanálů ve správci front LONDON, dokud se kanály nezastaví:

```
DISPLAY CHSTATUS(INVENTORY.LONDON)
DISPLAY CHSTATUS(INVENTORY.TORONTO)
DISPLAY CHSTATUS(INVENTORY.PARIS)
DISPLAY CHSTATUS(INVENTORY.NEWYORK)
```

   Po zastavení kanálů nejsou do ostatních správců front v klastru ani z nich odesílány žádné další zprávy aplikace.

4. Odstraňte ručně definované kanály klastru ve správci front LONDON:

```
DELETE CHANNEL(INVENTORY.NEWYORK)
DELETE CHANNEL(INVENTORY.TORONTO)
```

5. Zbývající správci front v klastru stále uchovávají informace o odebraném správci front a mohou do něj nadále odesílat zprávy. Chcete-li vymazat informace ze zbývajících správců front, resetujte odebraného správce front z klastru v jednom z úplných úložišť:

```
RESET CLUSTER(INVENTORY) ACTION(FORCEREMOVE) QMNAME(LONDON) QUEUES(YES)
```

   Pokud v klastru existuje jiný správce front, který má stejný název jako odebraný správce front, zadejte hodnotu **QMID** odebraného správce front.

Výsledky

Správce front LONDON již není součástí klastru. Může však i nadále fungovat jako nezávislý správce front.

Jak pokračovat dále

Výsledek těchto změn lze potvrdit zadáním následujícího příkazu na zbývajících členech klastru:

```
DISPLAY CLUSQMGR(LONDON)
```

Správce front se bude nadále zobrazovat, dokud se automaticky definované odesílací kanály klastru nezastaví. Můžete počkat, až k tomu dojde, nebo pokračovat v monitorování aktivních instancí zadáním následujícího příkazu:

```
DISPLAY CHANNEL(INVENTORY.LONDON)
```

Po rozšíření změn v rámci klastru a po nedoručení dalších zpráv do tohoto správce front odstraňte kanál CLUSRCVR v systému LONDON:

```
DELETE CHANNEL(INVENTORY.LONDON)
```

Odebraného správce front lze později přidat zpět do klastru, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 308. Odebraný správce front bude nadále ukládat do mezipaměti informace o zbývajících členech klastru po dobu až 90 dnů. Pokud nechcete čekat na vypršení platnosti této mezipaměti, můžete ji vynuceně odebrat, jak je popsáno v tématu “Obnovení správce front do stavu před klastrem” na stránce 357.

Související odkazy

DELETE CHANNEL (odstranění kanálu)

DISPLAY CHANNEL (zobrazit definici kanálu)

DISPLAY CHSTATUS (zobrazení stavu kanálu)

DISPLAY CLUSQMGR (zobrazit informace o kanálu pro správce front klastru)

STOP CHANNEL (zastavení kanálu)

RESET CLUSTER (resetujte klastr)

Obnovení správce front do stavu před klastrem

Pokud je správce front odebrán z klastru, zachovává si informace o zbývajících členech klastru. Tato znalost nakonec vyprší a je automaticky vymazána. Pokud však dáváte přednost okamžitému odstranění, můžete použít kroky uvedené v tomto tématu.

Než začnete

Předpokládá se, že správce front byl odebrán z klastru a již neprovádí žádnou práci v klastru. Například jeho fronty již nepřijímají zprávy z klastru a žádné aplikace nečekají na doručení zpráv do těchto front.

Informace o této úloze

Když je správce front odebrán z klastru, uchová si informace o zbývajících členech klastru až po dobu 90 dnů. To může mít systémové výhody, zejména pokud se správce front rychle znovu připojí ke klastru. Po vypršení platnosti těchto znalostí dojde k jejich automatickému odstranění. Existují však důvody, proč byste mohli raději odstranit tyto informace ručně. Příklad:

- Možná budete chtít potvrdit, že jste zastavili všechny aplikace v tomto správci front, které dříve používaly prostředky klastru. Dokud nevyprší platnost znalostí o zbývajících členech 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.
- Při zobrazení informací o stavu pro správce front může být lepší nezobrazovat informace o zbývajících členech klastru, jejichž platnost vyprší.

Tato úloha používá klastr INVENTORY jako příklad. Správce front LONDON byl odebrán z klastru INVENTORY , jak je popsáno v tématu “Odebrání správce front z klastru: doporučený postup” na stránce 353. Chcete-li odstranit informace o zbývajících členech klastru, zadejte ve správci front 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 ztraceny:

```
DISPLAY CLUSQMGR(*) CLUSTER(INVENTORY)
DISPLAY QCLUSTER(*) CLUSTER(INVENTORY)
DISPLAY TOPIC(*) CLUSTER(INVENTORY)
```

Související pojmy

Klastry

Komponenty klastru

Související odkazy

Porovnání klastrování a distribuovaného řazení do front

Údržba správce front

Pozastavte a obnovte správce front z klastru za účelem provedení údržby.

Informace o této úloze

Čas od času může být nutné provést údržbu správce front, který je součástí klastru. Můžete například potřebovat provést zálohování dat v jeho frontách nebo použít opravy na software. Pokud je správce front hostitelem front, musí být jeho aktivity pozastaveny. Po dokončení údržby lze její aktivity obnovit.

Postup

1. Pozastavte správce front zadáním příkazu SUSPEND QMGR **runmqsc** :

```
SUSPEND QMGR CLUSTER(SALES)
```

   Příkaz SUSPEND **runmqsc** oznámí správcům front v klastru SALES , že byl tento správce front pozastaven.

   Účelem příkazu SUSPEND QMGR je pouze poradit ostatním správcům front, aby pokud možno neodesílali zprávy tomuto správci front. Neznamená to, že je správce front zakázán. Některé zprávy, které mají být zpracovány tímto správcem front, jsou mu stále odesílány, například pokud je tento správce front jediným hostitelem klastrované fronty.

   Zatímco je správce front pozastaven, rutiny správy pracovní zátěže mu neodesílají zprávy. Zprávy, které musí být zpracovány tímto správcem front, zahrnují zprávy odeslané lokálním správcem front.

   Produkt IBM MQ používá algoritmus vyrovnávání pracovní zátěže k určení, která místa určení jsou vhodná, a nikoli k výběru lokálního správce front, kdykoli je to možné.

   a) Vynuťte pozastavení správce front pomocí volby FORCE v příkazu SUSPEND QMGR :

```
SUSPEND QMGR CLUSTER(SALES) MODE(FORCE)
```

      Produkt MODE(FORCE) vynuceně zastaví všechny příchozí kanály od ostatních správců front v klastru. Pokud neuvedete MODE(FORCE), použije se výchozí hodnota MODE(QUIESCE) .

2. Proveďte všechny nezbytné úlohy údržby.
3. Obnovte činnost správce front zadáním příkazu RESUME QMGR **runmqsc** :

```
RESUME QMGR CLUSTER(SALES)
```

Výsledky

Příkaz RESUME **runmqsc** oznámí úplným úložištím, že je správce front znovu k dispozici. Správci front úplného úložiště tyto informace rozšiřují mezi další správce front, kteří požadovali aktualizace informací týkajících se tohoto správce front.

Údržba přenosové fronty klastru

Vynaložit veškeré úsilí na to, aby byly přenosové fronty klastru k dispozici. Jsou nezbytné pro výkon klastrů. z/OS V systému z/OSnastavte INDXTYPE přenosové fronty klastru na hodnotu CORRELID.

Než začnete

- Ujistěte se, že přenosová fronta klastru není plná.
- Dbejte na to, abyste nezadali příkaz ALTER **runmqsc** k jeho nastavení, buď jej vypněte, nebo omylem vypněte.
- Ujistěte se, že médium, na kterém je přenosová fronta klastru uložena, z/OS (například z/OS sady stránek) není plné.

Informace o této úloze

z/OS

Následující postup platí pouze pro z/OS.

Postup

Nastavte parametr INDXTYPE přenosové fronty klastru na hodnotu CORRELID .

Aktualizace správce front klastru

Pomocí příkazu REFRESH CLUSTER můžete odebrat automaticky definované kanály a automaticky definované objekty klastru z lokálního úložiště. Žádné zprávy nejsou ztraceny.

Než začnete

Můžete být požádáni, abyste příkaz použili ve svém Centru podpory IBM . Nepoužívejte příkaz bez pečlivého uvážení. V případě velkých klastrů může být například použití příkazu **REFRESH CLUSTER** pro probíhající klastr s přerušením a poté znovu v 27 denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zainteresovaným správcům front. Viz Klastrování: Použití doporučených postupů REFRESH CLUSTER.

Informace o této úloze

Správce front může provést nový start v klastru. Za normálních okolností nemusíte používat příkaz REFRESH CLUSTER .

Postup

Zadáním příkazu REFRESH CLUSTER **MQSC** ze správce front odeberte automaticky definovaného správce front klastru a objekty front z lokálního úložiště.

Příkaz odebere pouze objekty, které odkazují na jiné správce front, neodebere objekty související s lokálním správcem front. Příkaz také odebere automaticky definované kanály. Odebere kanály, které nemají zprávy v přenosové frontě klastru a nejsou připojeny ke správci front úplného úložiště.

Výsledky

Příkaz REFRESH CLUSTER efektivně umožňuje spuštění správce front za studena s ohledem na jeho úplný obsah úložiště. Produkt IBM MQ zajišťuje, že z front nebudou ztracena žádná data.

Související informace

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Obnova správce front klastru

Pomocí příkazu REFRESH CLUSTER **runmqsc** můžete aktualizovat informace o klastru o správci front. Postupujte podle tohoto postupu po obnovení správce front ze zálohy k určitému okamžiku.

Než začnete

Obnovili jste správce front klastru ze zálohy k určitému okamžiku.

Informace o této úloze

Chcete-li obnovit správce front v klastru, obnovte jej a poté pomocí příkazu REFRESH CLUSTER **runmqsc** obnovte informace o klastru.

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

Postup

Zadejte příkaz REFRESH CLUSTER pro obnoveného správce front pro všechny klastry, ve kterých je správce front zapojen.

Jak pokračovat dále

Není třeba zadat příkaz REFRESH CLUSTER pro žádného jiného správce front.

Související pojmy

Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Konfigurace kanálů klastru pro dostupnost

Postupujte podle osvědčených postupů konfigurace, aby kanály klastru fungovaly hladce, pokud dojde k přerušovaným síťovým odstávkám.

Než začnete

Klastry vás zbavují nutnosti definovat kanály, ale stále je třeba je udržovat. Stejná technologie kanálu se používá pro komunikaci mezi správci front v klastru jako v distribuovaném řazení do front. Chcete-li porozumět kanálům klastru, musíte být obeznámeni s takovými záležitostmi, jako jsou:

- Jak kanály fungují
- Jak zjistit jejich stav
- Jak používat uživatelské procedury kanálu

Informace o této úloze

Možná budete chtít 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 spoustou prezenčního signálu nebo neudržují aktivní toky. Interval menší než asi 10 sekund dává nepravdivá selhání, pokud vaše síť někdy zpomaluje a zavádí zpoždění této délky.
- Nastavte hodnotu BATCHHB tak, aby se zmenšilo okno pro vyvolání marooned zprávy, protože se jedná o nejistý kanál, pro který došlo k selhání. Nejistá dávka na nezdařeném kanálu se pravděpodobně vyskytne, pokud je dávková dávka delší, aby se naplnila. Pokud je přenos zpráv podél kanálu

sporadický s dlouhým časovým obdobím mezi shluky zpráv, je pravděpodobnější, že dojde k selhání dávky.

- K problému dojde, pokud dojde k selhání odesílacího konce kanálu klastru a poté se pokusí o restart dříve, než prezenční signál nebo udržení aktivity zjistí selhání. Restart odesílatele kanálu je odmítnut v případě, že konec přijímacího kanálu klastru zůstal aktivní. Chcete-li se vyhnout selhání, zařiďte, aby byl kanál příjemce klastru ukončen a restartován při pokusu kanálu odesilatele klastru o restart.

  z/OS **zapIBM MQ for z/OS**

  Pomocí parametrů **ADOPTMCA** a **ADOPTCHK** na serveru **ALTER QMGR**můžete řídit problém s koncem přijímače klastru kanálu, který zůstává aktivní.

  Multi **zapMultiplatforms**

  Pomocí atributů **AdoptNewMCA**, **AdoptNewMCATimeout**a **AdoptNewMCACheck** v souboru qm.ini nebo v registru Windows můžete řídit problém s koncem přijímače klastru kanálu, který zůstává aktivní.

Příklad

Příklady implementace těchto nastavení v systémech IBM MQ for z/OS a IBM MQ for Multiplatformsnaleznete v části “Navrhovaná nastavení” na stránce 227 .

Kontrola dokončení asynchronních příkazů pro distribuované sítě

Mnoho příkazů je při použití v distribuované síti asynchronních. V závislosti na příkazu a stavu sítě, když je vydán, může trvat delší dobu, než se dokončí. Správce front při dokončení nevydá zprávu, takže potřebujete jiné způsoby, jak zkontrolovat, zda byl příkaz dokončen.

Informace o této úloze

Téměř každá změna konfigurace, kterou provedete v klastru, bude pravděpodobně dokončena asynchronně. Důvodem jsou interní cykly administrace a aktualizace, které fungují v rámci klastrů. V případě hierarchií publikování/odběru je pravděpodobné, že všechny změny konfigurace, které ovlivňují odběry, budou dokončeny asynchronně. To není vždy zřejmé z názvu příkazu.

Následující příkazy MQSC mohou být dokončeny asynchronně. Každý z těchto příkazů má ekvivalent PCF a většina z nich je také k dispozici v rámci produktu IBM MQ Explorer . Při spuštění v malé síti bez pracovní zátěže jsou tyto příkazy obvykle dokončeny během několika sekund. To však není případ větších a rušnějších sítí. Příkaz **REFRESH CLUSTER** může také trvat mnohem déle, zejména pokud je zadán ve více správcích front současně.

Chcete-li mít jistotu, že tyto příkazy byly dokončeny, zkontrolujte, zda ve vzdálených správcích front existují očekávané objekty.

Procedura

- ALTER QMGR

  Pro příkaz ALTER QMGR PARENT použijte příkaz DISPLAY PUBSUB TYPE(PARENT) ALL ke sledování stavu požadovaného nadřízeného vztahu.

  Pro příkazy ALTER QMGR REPOS a ALTER QMGR REPOSNL použijte příkaz DISPLAY CLUSQMGR QMTYPE k potvrzení dokončení.

- DEFINE CHANNEL, ALTER CHANNELa DELETE CHANNEL

  Pro všechny parametry uvedené v tabulce ALTER CHANNEL parameterspoužijte příkaz DISPLAY CLUSQMGR k monitorování, kdy byly změny rozšířeny do klastru.

- DEFINE NAMELIST, ALTER NAMELISTa DELETE NAMELIST.

  Pokud použijete parametr **NAMELIST** na atributu **CLUSNL** objektu **QMgr** , může tento objekt ovlivnit fronta nebo kanál klastru. Monitorujte podle potřeby pro ovlivněný objekt.

Změny v souboru SYSTEM.QPUBSUB.QUEUE.NAMELIST mohou ovlivnit vytvoření nebo zrušení proxy odběrů v hierarchii publikování/odběru. K monitorování použijte příkaz DISPLAY SUB SUBTYPE(PROXY) .

- Fronty DEFINE, fronty ALTERa fronty DELETE.

  Pro všechny parametry uvedené v tabulce Parametry, které lze vrátit příkazem DISPLAY QUEUE, použijte příkaz DISPLAY QCLUSTER k monitorování, kdy byly změny rozšířeny do klastru.

- DEFINE SUBa DELETE SUB

  Při definování prvního odběru v řetězci tématu můžete vytvořit proxy odběry v hierarchii publikování/odběru nebo v klastru publikování/odběru. Podobně, když odstraníte poslední odběr v řetězci tématu, můžete zrušit proxy odběry v hierarchii publikování/odběru nebo v klastru publikování/odběru.

  Chcete-li zkontrolovat, zda byl dokončen příkaz definující nebo odstraňující odběr, zkontrolujte, zda očekávaný proxy odběr existuje v jiných správcích front v distribuované síti. Používáte-li v klastru *přímé směrování* , zkontrolujte, zda očekávaný proxy odběr existuje v ostatních dílčích úložištích v klastru. Používáte-li v klastru *směrování hostitelů témat* , zkontrolujte, zda v odpovídajících hostitelích témat existuje očekávaný proxy odběr. Použijte následující příkaz MQSC:

  ```
  DISPLAY SUB(*) SUBTYPE(PROXY)
  ```

  Použijte stejnou kontrolu pro následující ekvivalentní volání MQI pro odběr a zrušení odběru, když jsou vydána v klastru nebo hierarchii:

  – Přihlaste se k odběru pomocí MQSUB.
  – Zrušte odběr pomocí příkazu MQCLOSE s parametrem MQCO_REMOVE_SUB.

- DEFINE TOPIC, ALTER TOPICa DELETE TOPIC

  Chcete-li zkontrolovat, že příkaz definující, měnící nebo odstraňující klastrované téma byl dokončen, zobrazte téma v ostatních dílčích úložištích v klastru (pokud používáte *přímé směrování*). nebo v jiných hostitelích témat (pokud používáte *směrování hostitelů témat*).

  Pro všechny parametry uvedené v tabulce Parametry, které mohou být vráceny příkazem DISPLAY TOPIC, použijte příkaz DISPLAY TCLUSTER k monitorování, kdy byly změny rozšířeny do klastru.

  Poznámka:

  – Parametr **CLUSTER** může ovlivnit vytvoření nebo zrušení proxy odběrů v klastru publikování/odběru.
  – Parametry **PROXYSUB** a **SUBSCOPE** mohou ovlivnit vytvoření nebo zrušení proxy odběrů v hierarchii publikování/odběru nebo v klastru publikování/odběru.
  – K monitorování použijte příkaz DISPLAY SUB SUBTYPE(PROXYSUB) .

- Aktualizovat klastr

  Pokud spouštíte příkaz **REFRESH CLUSTER** , vyzývat hloubku fronty příkazů klastru. Před hledáním objektů počkejte, až dosáhne nuly, a zůstaňte na nule.

  1. Pomocí následujícího příkazu MQSC zkontrolujte, zda je hloubka fronty příkazů klastru nulová.

     ```
     DISPLAY QL(SYSTEM.CLUSTER.COMMAND.QUEUE) CURDEPTH
     ```

  2. Opakujte kontrolu, dokud hloubka fronty nedosáhne nuly, a v následné kontrole zůstane na nule.

  Příkaz **REFRESH CLUSTER** odebere a znovu vytvoří objekty a dokončení ve velkých konfiguracích může trvat delší dobu. Viz Aspekty REFRESH CLUSTER pro klastry publikování/odběru.

- REFRESH QMGR TYPE (PROXYSUB)

  Chcete-li zkontrolovat, zda byl příkaz **REFRESH QMGR TYPE(PROXYSUB)** dokončen, zkontrolujte, zda byly proxy odběry opraveny v jiných správcích front v distribuované síti. Používáte-li v klastru *přímé směrování* , zkontrolujte, zda byly proxy odběry opraveny v ostatních dílčích úložištích v klastru.

Používáte-li v klastru *směrování hostitelů témat* , zkontrolujte, zda byly očekávané proxy odběry opraveny na odpovídajících hostitelích témat. Použijte následující příkaz MQSC:

```
DISPLAY SUB(*) SUBTYPE(PROXYSUB)
```

- Reset klastru

  Chcete-li zkontrolovat, zda byl příkaz **RESET CLUSTER** dokončen, použijte `DISPLAY CLUSQMGR`.
- RESET QMGR TYPE (PUBSUB)

  Chcete-li zkontrolovat, zda byl příkaz **RESET QMGR** dokončen, použijte `DISPLAY PUBSUB TYPE(PARENT|CHILD)`.

  Poznámka: Příkaz **RESET QMGR** může způsobit zrušení proxy odběrů v hierarchii publikování/odběru nebo v klastru publikování/odběru. K monitorování použijte příkaz `DISPLAY SUB SUBTYPE(PROXYSUB)` .
- Můžete také monitorovat další systémové fronty, které po dokončení příkazů směřují k nulové hloubce fronty.

  Můžete například monitorovat frontu `SYSTEM.INTER.QMGR.CONTROL` a frontu `SYSTEM.INTER.QMGR.FANREQ` . Viz Monitorování provozu proxy odběrů v klastrech a Vyvažování producentů a spotřebitelů v sítích publikování/odběru.

Jak pokračovat dále

Pokud tyto kontroly nepotvrdí, že asynchronní příkaz byl dokončen, mohlo dojít k chybě. Chcete-li provést vyšetření, nejprve zkontrolujte protokol pro správce front, pro kterého byl příkaz zadán, a poté (pro klastr) zkontrolujte protokoly úplného úložiště klastru.

Související odkazy

z/OS Asynchronní chování příkazů CLUSTER v systému z/OS

Směrování zpráv do klastrů a z klastrů

Pomocí aliasů front, aliasů správců front a definic vzdálených front můžete připojovat klastry k externím správcům front a dalším klastrům.

Podrobnosti o směrování zpráv do klastrů a z klastrů naleznete v následujících dílčích tématech:

Související pojmy

Klastry

Komponenty klastru

“Aliasy a klastry správce front” na stránce 377
Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

“Aliasy front a klastry” na stránce 380
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

“Aliasy a klastry fronty pro odpovědi” na stránce 379
Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Související úlohy

“Konfigurace klastru správců front” na stránce 284
Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

“Nastavení nového klastru” na stránce 297
Postupujte podle těchto pokynů, abyste nastavili ukázkový klastr. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosovými frontami. Otestujte práci klastru odesláním zprávy z jednoho správce front do druhého.

Související odkazy

Porovnání klastrování a distribuovaného řazení do front

Konfigurace požadavku/odpovědi na klastr

Nakonfigurujte cestu ke zprávě požadavku/odpovědi ze správce front mimo klastr. Skrytí vnitřních podrobností klastru pomocí správce front brány jako komunikační cesty do klastru a z klastru.

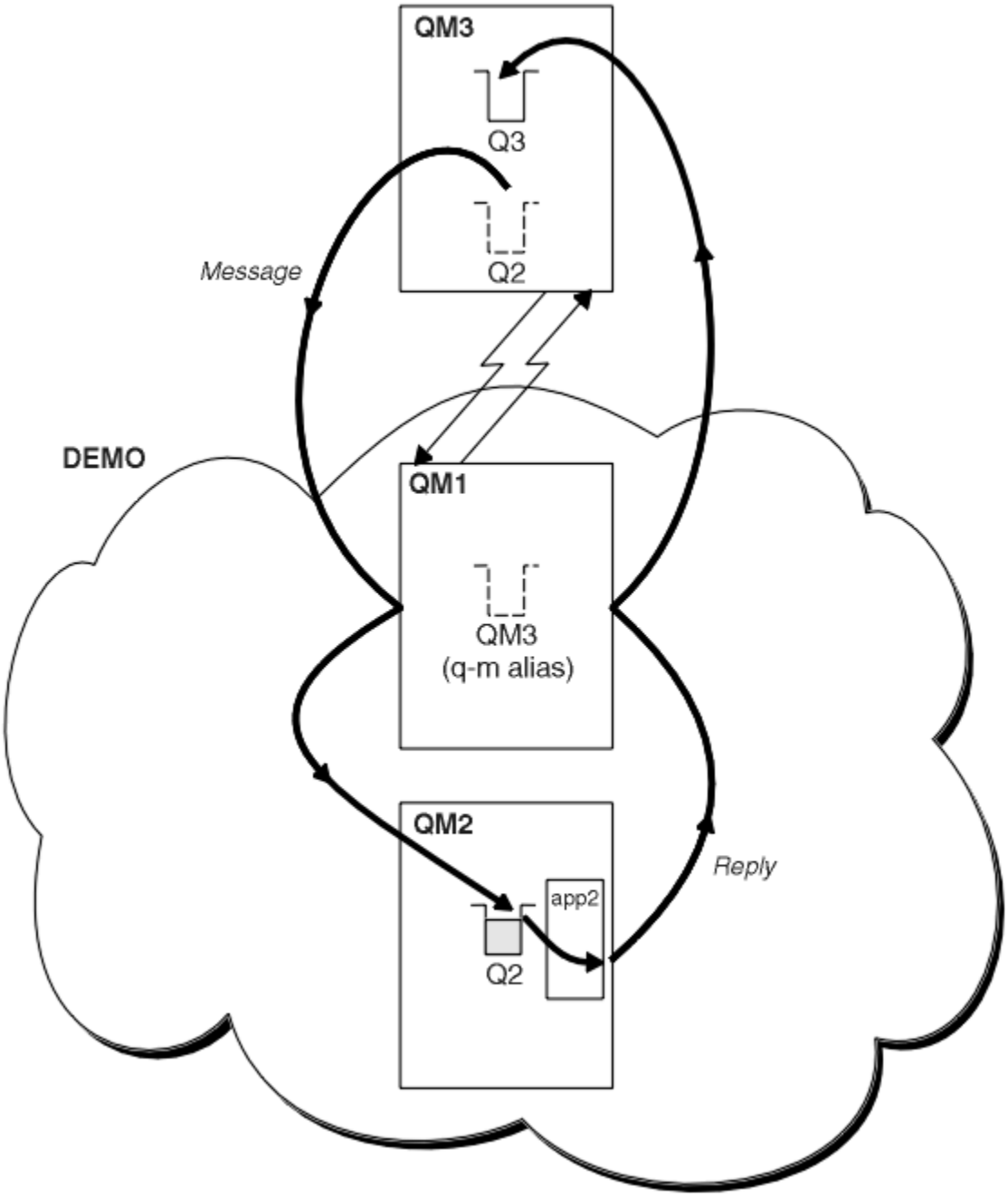
Než začnete

Obrázek 53 na stránce 365 zobrazuje správce front s názvem QM3 , který je mimo klastr s názvem DEMO. QM3 může být správcem front v produktu IBM MQ , který nepodporuje klastry. QM3 je hostitelem fronty s názvem Q3, která je definována takto:

```
DEFINE QLOCAL(Q3)
```

V klastru jsou dva správci front s názvem QM1 a QM2. QM2 je hostitelem fronty klastru s názvem Q2, která je definována takto:

```
DEFINE QLOCAL(Q2) CLUSTER(DEMO)
```



Obrázek 53. Vložení ze správce front mimo klastr

Informace o této úloze

Postupujte podle doporučení v proceduře a nastavte cestu pro zprávy požadavku a odpovědi.

Postup

1. Odešlete zprávu požadavku do klastru.

   Zvažte, jak správce front, který je mimo klastr, vloží zprávu do fronty Q2 v QM2, která je uvnitř klastru. Správce front mimo klastr musí mít pro každou frontu v klastru, do které vkládá zprávy, definici QREMOTE .

   a) Definujte vzdálenou frontu pro Q2 na QM3.

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(QM2) XMITQ(QM1)
```

Protože produkt QM3 není součástí klastru, musí komunikovat pomocí technik distribuovaného řazení do front. Proto musí mít také odesílací kanál a přenosovou frontu do produktu QM1. Produkt QM1 potřebuje odpovídající přijímací kanál. Kanály a přenosové fronty nejsou v souboru Obrázek 53 na stránce 365zobrazeny explicitně.

V příkladu aplikace v QM3 vydá volání MQPUT pro vložení zprávy do Q2. Definice QREMOTE způsobí, že zpráva bude směrována do Q2 v QM2 pomocí odesílacího kanálu, který získává zprávy z přenosové fronty QM1 .

2. Přijměte zprávu odpovědi z klastru.

   Použijte alias správce front k vytvoření návratové cesty pro odpovědi na správce front mimo klastr. Brána QM1propaguje alias správce front pro správce front, který je mimo klastr QM3. Inzeruje produkt QM3 správcům front v rámci klastru přidáním atributu klastru do definice aliasu správce front pro produkt QM3. Definice aliasu správce front je jako definice vzdálené fronty, ale s prázdným RNAME.

   a) Definujte alias správce front pro QM3 on QM1.

   ```
   DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
   ```

   Musíme zvážit volbu názvu pro přenosovou frontu používanou k předávání odpovědí zpět z QM1 do QM3. Implicitní v definici QREMOTE při vynechání atributu XMITQ je název přenosové fronty QM3. Ale QM3 je stejný název, jaký očekáváme, že budeme ostatním klastru nabízet pomocí aliasu správce front. Produkt IBM MQ neumožňuje zadat pro přenosovou frontu a alias správce front stejný název. Jedním řešením je vytvořit přenosovou frontu pro předávání zpráv do produktu QM3 s jiným názvem do aliasu správce front.

   b) Zadejte název přenosové fronty v definici QREMOTE .

   ```
   DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO) XMITQ(QM3.XMIT)
   ```

   Nový alias správce front spojí novou přenosovou frontu s názvem QM3.XMIT s aliasem správce front QM3 . Je to jednoduché a správné řešení, ale ne zcela uspokojivé. Porušila konvenci pojmenování pro přenosové fronty, které mají stejný název jako cílový správce front. Existují alternativní řešení, která zachovávají konvenci pojmenování přenosové fronty?

   Problém se vyskytl, protože žadatel standardně předal QM3 jako název správce front pro odpověď ve zprávě požadavku, která je odeslána z QM3. Server v systému QM2 používá ve svých odpovědích QM3 název správce front pro odpovědi k adresování QM3 . Řešení vyžadovalo, aby produkt QM1 propagoval QM3 jako alias správce front pro vrácení zpráv s odpovědí do produktu QM1 a zabránil mu v použití produktu QM3 jako názvu přenosové fronty.

   Místo toho, aby aplikace v systému QM3 standardně poskytovaly jako název správce front pro odpovědi QM3 , musí pro zprávy odpovědí předat alias správce front pro odpovědi QM1 . Správce front brány QM1 inzeruje alias správce front pro odpovědi na QM3 spíše než QM3 sám, čímž se vyhne konfliktu s názvem přenosové fronty.

   c) Definujte alias správce front pro QM3 on QM1.

   ```
   DEFINE QREMOTE(QM3.ALIAS) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
   ```

   Jsou vyžadovány dvě změny konfiguračních příkazů.

   i) QREMOTE at QM1 nyní inzeruje alias našeho správce front QM3.ALIAS zbytku klastru a spojí jej s názvem skutečného správce front QM3. QM3 je opět název přenosové fronty pro odeslání front odpovědí zpět do QM3

ii) Klientská aplikace musí při vytváření zprávy požadavku zadat jako název správce front pro odpovědi hodnotu `QM3.ALIAS` . Aplikaci klienta můžete poskytnout `QM3.ALIAS` jedním ze dvou způsobů.

- Kód `QM3.ALIAS` v poli názvu správce front pro odpověď sestaveném pomocí `MQPUT` v souboru `MQMD`. Musíte to provést tímto způsobem, pokud používáte dynamickou frontu pro odpovědi.
- Při zadávání názvu fronty pro odpověď použijte alias fronty pro odpověď, `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 pro odpovědi s **AMQSREQ0**. Otevře frontu pro odpověď s použitím názvu fronty uvedeného v parametru 3 nebo výchozí modelové fronty `SYSTEM.SAMPLE.REPLY` . Je třeba upravit ukázku a zadat další parametr obsahující alias fronty pro odpověď, který bude pojmenovat alias správce front pro odpověď pro `MQPUT`.

Související pojmy

Aliasy a klastry správce front
Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

Aliasy a klastry fronty pro odpovědi
Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Aliasy front a klastry
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě požadavku/odpovědi z klastru do správce front mimo klastr. Skrýt podrobnosti o způsobu, jakým správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

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.

“Skrytí názvu správce cílových front klastru” na stránce 367
Směrovat zprávu do fronty klastru, která je definována v libovolném správci front v klastru bez pojmenování správce front.

Skrytí názvu správce cílových front klastru
Směrovat zprávu do fronty klastru, která je definována v libovolném správci front v klastru bez pojmenování správce front.

Než začnete

- Vyhněte se zobrazení názvů správců front, kteří jsou v klastru, správcům front, kteří jsou mimo klastr.
  - 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 proměnnou `RQMNAME` aliasem správce front poskytnutým administrátorem klastru.

  - “Skrytí názvu správce cílových front klastru” na stránce 367 popisuje použití aliasu správce front k oddělení správce front mimo klastr od správy správců front v klastru.
- Navrhovaným způsobem, jak pojmenovat přenosové fronty, je dát jim název cílového správce front. Název přenosové fronty zobrazuje název správce front v klastru. Musíte si vybrat, které pravidlo následovat. Přenosovou frontu můžete pojmenovat buď pomocí názvu správce front, nebo pomocí názvu klastru:

  Pojmenujte přenosovou frontu pomocí názvu správce front brány
  Předání názvu správce front brány správcům front mimo klastr představuje rozumnou výjimku z pravidla skrytí názvů správců front klastru.

  Pojmenujte přenosovou frontu pomocí názvu klastru.
  Pokud nedodržujete konvenci pojmenování přenosových front s názvem cílového správce front, použijte název klastru.

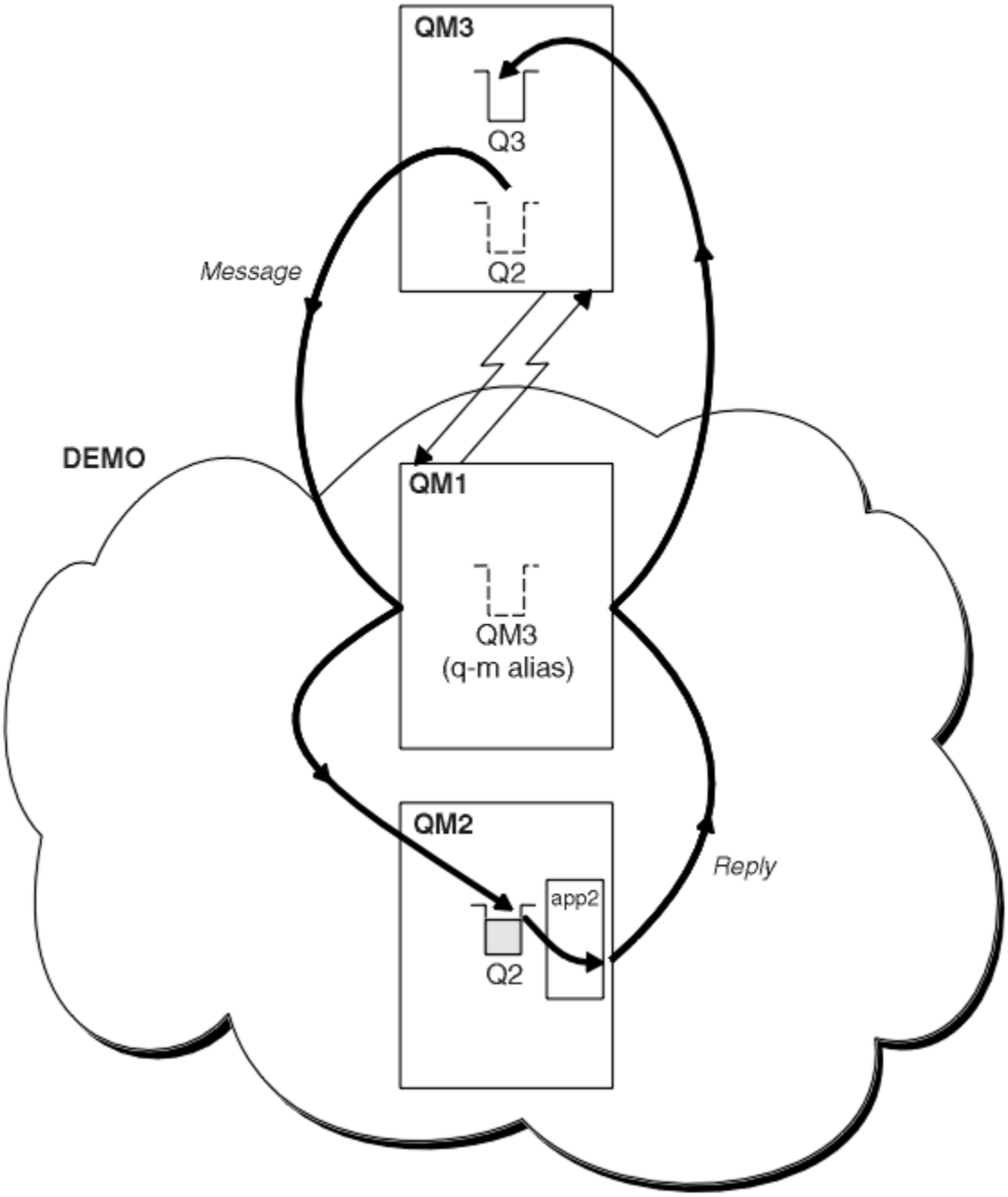
Informace o této úloze

Upravte úlohu “Konfigurace požadavku/odpovědi na klastr” na stránce 364, abyste skryli název cílového správce front v klastru.

Postup

V tomto příkladu viz Obrázek 54 na stránce 369, definujte alias správce front ve správci front brány QM1 s názvem DEMO:

```
DEFINE QREMOTE(DEMO) RNAME(' ') RQMNAME(' ')
```



Obrázek 54. Vložení ze správce front mimo klastr

Definice QREMOTE v systému QM1 uvádí alias správce front DEMO pro správce front brány. QM3, Správce front mimo klastr může používat alias správce front DEMO k odesílání zpráv do front klastru v systému DEMO, aniž by musel používat skutečný název správce front.

Pokud přijmete konvenci použití názvu klastru k pojmenování přenosové fronty připojující se ke klastru, bude definice vzdálené fronty pro Q2 následující:

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(DEMO) XMIT(DEMO)
```

Výsledky

Zprávy určené pro Q2 on DEMO jsou umístěny do přenosové fronty DEMO . Z přenosové fronty jsou přeneseny odesílacím kanálem do správce front brány QM1. Správce front brány směruje zprávy na všechny správce front v klastru, který je hostitelem fronty klastru Q2.

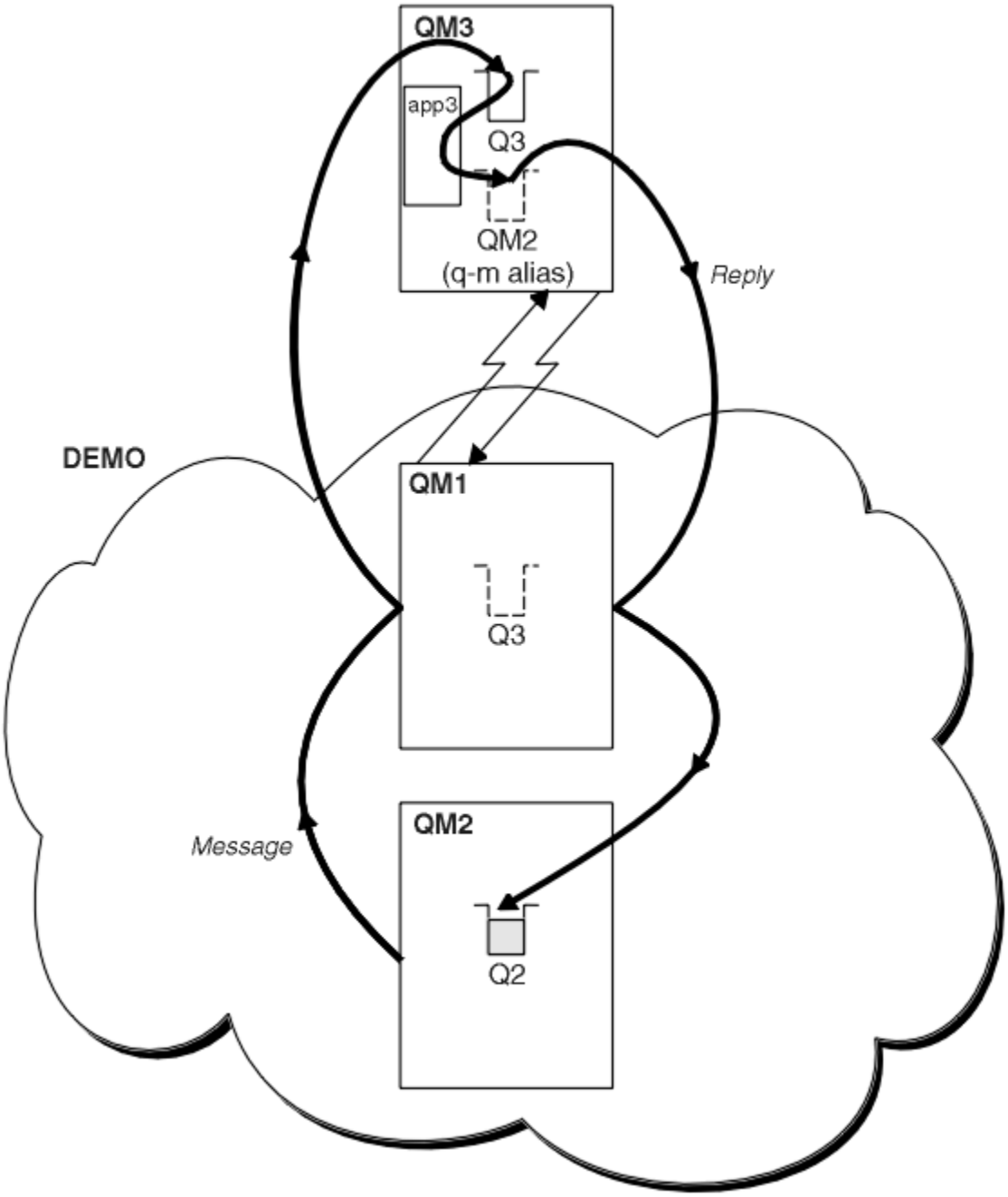
Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě požadavku/odpovědi z klastru do správce front mimo klastr. Skrýt podrobnosti o způsobu, jakým správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Než začnete

Obrázek 55 na stránce 371 zobrazuje správce front QM2uvnitř klastru DEMO. Odešle požadavek do fronty Q3, jejímž hostitelem je správce front mimo klastr. Odpovědi se vrátí na Q2 at QM2 uvnitř klastru.

Chcete-li komunikovat se správcem front mimo klastr, jeden nebo více správců front v klastru vystupuje jako brána. Správce front brány má komunikační cestu ke správcům front mimo klastr. V příkladu je brána QM1 .



Obrázek 55. Vložení 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, jak správce front QM2, který je uvnitř klastru, vloží zprávu do fronty Q3 v QM3, která je mimo klastr.

   a) Vytvořte definici QREMOTE v systému QM1 , která bude do klastru inzerovat vzdálenou frontu Q3 .

```
DEFINE QREMOTE(Q3) RNAME(Q3) RQMNAME(QM3) CLUSTER(DEMO)
```

Má také odesílací kanál a přenosovou frontu na správce front, který je mimo klastr. QM3 má odpovídající přijímací kanál. Kanály nejsou zobrazeny v souboru Obrázek 55 na stránce 371.

Aplikace v systému QM2 vydá volání MQPUT uvádějící cílovou frontu a frontu, do které mají být odesílány odpovědi. Cílová fronta je Q3 a fronta pro odpověď je Q2.

Zpráva je odeslána do adresáře QM1, který používá svou definici vzdálené fronty k vyřešení názvu fronty na Q3 at QM3.

2. Přijměte zprávu odpovědi od správce front mimo klastr.

   Správce front mimo klastr musí mít alias správce front pro každého správce front v klastru, kterému odesílá zprávu. Alias správce front musí také určovat název přenosové fronty pro správce front brány. V tomto příkladu produkt QM3 potřebuje definici aliasu správce front pro 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 QM1 a QM1 potřebuje odpovídající přijímací kanál.

   Aplikace **app3**v systému QM3 poté může odesílat odpovědi na adresu QM2zadáním volání MQPUT a zadáním názvu fronty Q2 a názvu správce front QM2.

Jak pokračovat dále

Můžete definovat více než jednu trasu mimo klastr.

Související pojmy

Aliasy a klastry správce front
Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

Aliasy a klastry fronty pro odpovědi
Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Aliasy front a klastry
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr
Nakonfigurujte cestu ke zprávě požadavku/odpovědi ze správce front mimo klastr. Skrytí vnitřních podrobností klastru pomocí správce front brány jako komunikační cesty do klastru a z klastru.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

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.

Konfigurace vyrovnávání pracovní zátěže mimo klastr

Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

Než začnete

Nakonfigurujte příklad, jak ukazuje Obrázek 53 na stránce 365 v “Konfigurace požadavku/odpovědi na klastr” na stránce 364.

Informace o této úloze

V tomto scénáři správce front mimo klastr, QM3 v Obrázek 56 na stránce 374, odesílá požadavky do fronty Q2. Hostitelem produktu Q2 jsou dva správci front QM2 a QM4 v rámci klastru DEMO. Oba správci front jsou nakonfigurováni s výchozí volbou vazby NOTFIXED , aby bylo možné používat vyrovnávání pracovní zátěže. Požadavky od QM3, správce front mimo klastr, jsou odeslány do jedné z instancí Q2 až QM1.

Produkt QM3 není součástí klastru a komunikuje pomocí technik distribuovaného řazení do front. Musí mít odesílací kanál a přenosovou frontu na QM1. Produkt QM1 potřebuje odpovídající přijímací kanál. Kanály a přenosové fronty nejsou v souboru Obrázek 56 na stránce 374zobrazeny explicitně.

Procedura rozšiřuje příklad v části Obrázek 53 na stránce 365 v části "Konfigurace požadavku/odpovědi na klastr" na stránce 364.

Postup

1. Vytvořte definici QREMOTE pro Q2 on QM3.

   ```
   DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(Q3) XMITQ(QM1)
   ```

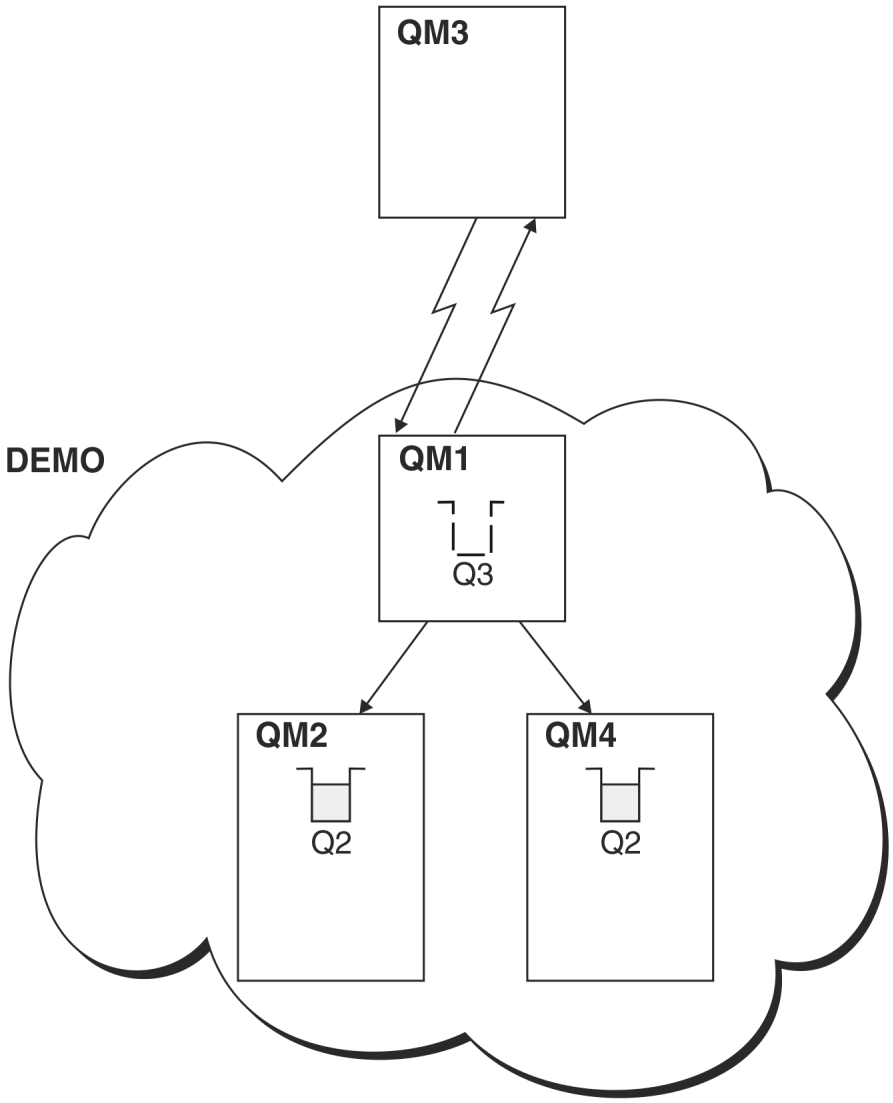
   Vytvořte definici QREMOTE pro každou frontu v klastru, do které QM3 vkládá zprávy.
2. Vytvořte alias správce front Q3 v systému QM1.

   ```
   DEFINE QREMOTE(Q3) RNAME(' ') RQMNAME(' ')
   ```

   Q3 není skutečný název správce front. Jedná se o název definice aliasu správce front v klastru, který odpovídá názvu aliasu správce front Q3 s mezerou, ' '
3. Definujte lokální frontu s názvem Q2 na každé z front QM2 a QM4.

   ```
   DEFINE QLOCAL(Q2) CLUSTER(DEMO) DEFBIND(NOTFIXED)
   ```
4. QM1, správce front brány, nemá žádné speciální definice.

Výsledky



Obrázek 56. Vložení ze správce front mimo klastr

Když aplikace QM3 vydá volání MQPUT pro vložení zprávy do systému Q2, definice QREMOTE v systému QM3 způsobí, že zpráva bude směrována prostřednictvím správce front brány QM1. Když produkt QM1 přijme zprávu, je si vědom, že zpráva je stále určena pro frontu s názvem Q2 a provádí rozlišování názvů. Produkt QM1 zkontroluje své lokální definice a nenalezne žádné pro Q2. Produkt QM1 poté zkontroluje konfiguraci svého klastru a zjistí, že má informace o dvou instancích Q2 v klastru DEMO. Produkt QM1 nyní může využívat vyrovnávání pracovní zátěže k distribuci zpráv mezi instancemi Q2 umístěnými na QM2 a QM4.

Související pojmy

Aliasy a klastry správce front
Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

Aliasy a klastry fronty pro odpovědi
Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Aliasy front a klastry
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

Rozlišení názvu

Související úlohy

Konfigurace požadavku/odpovědi na klastr
Nakonfigurujte cestu ke zprávě požadavku/odpovědi ze správce front mimo klastr. Skrytí vnitřních podrobností klastru pomocí správce front brány jako komunikační cesty do klastru a z klastru.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě požadavku/odpovědi z klastru do správce front mimo klastr. Skrýt podrobnosti o způsobu, jakým správce front v klastru komunikuje mimo klastr pomocí správce front brány.

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.

Související odkazy

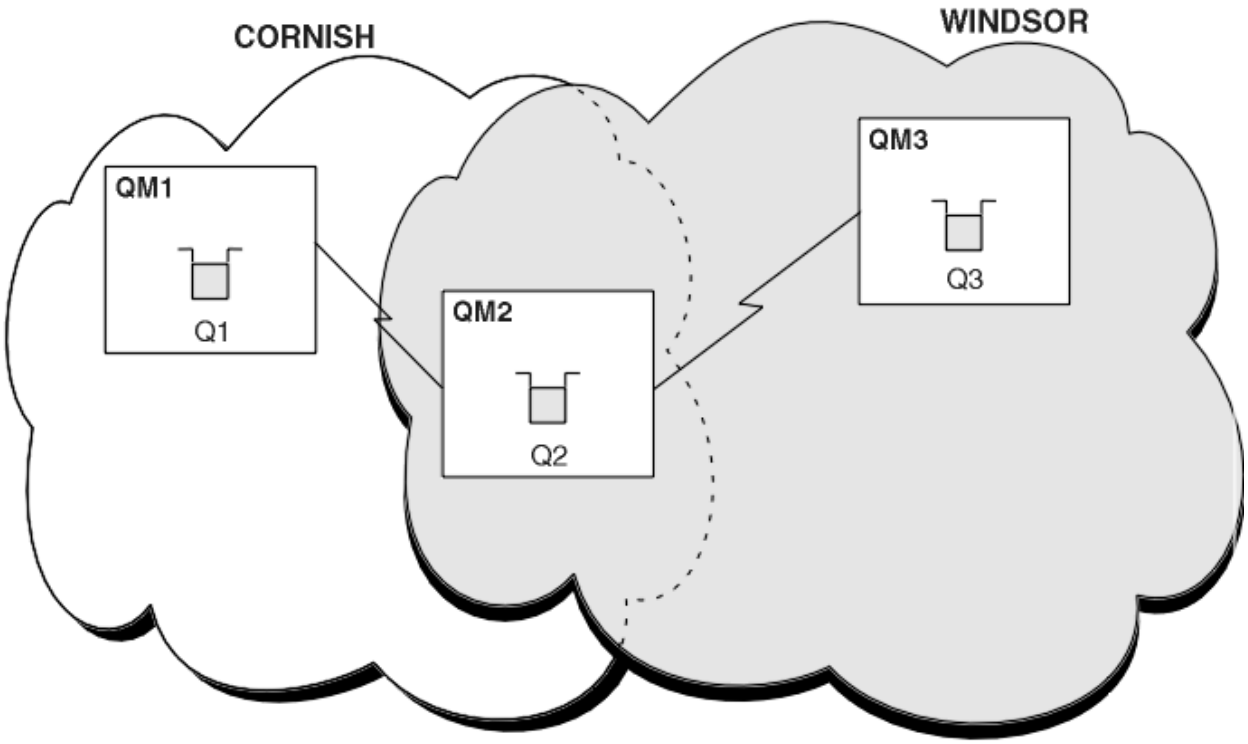
Rozlišení názvu fronty

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 Překrývající se klastry. Použijte aliasy ke změně názvů front a správců front, abyste se vyhnuli konfliktům názvů nebo abyste dodrželi místní konvence pojmenování.



Obrázek 57. Přemostění mezi klastry

Obrázek 57 na stránce 375 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 57 na stránce 375v 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 .

Související pojmy

Aliasy a klastry správce front
Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

Aliasy a klastry fronty pro odpovědi
Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Aliasy front a klastry
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr
Nakonfigurujte cestu ke zprávě požadavku/odpovědi ze správce front mimo klastr. Skrytí vnitřních podrobností klastru pomocí správce front brány jako komunikační cesty do klastru a z klastru.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě požadavku/odpovědi z klastru do správce front mimo klastr. Skrýt podrobnosti o způsobu, jakým správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

Aliasy a klastry správce front

Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

Aliasy správce front, které jsou vytvořeny pomocí definice vzdálené fronty s prázdným RNAME, mají pět použití:

Přemapování názvu správce front při odesílání zpráv

Alias správce front lze použít k opětovnému mapování názvu správce front určeného ve volání MQOPEN na jiného správce front. Může se jednat o správce front klastru. Správce front může mít například definici aliasu správce front:

```
DEFINE QREMOTE(YORK) RNAME(' ') RQMNAME(CLUSQM)
```

YORK lze použít jako alias pro správce front s názvem CLUSQM. Když aplikace ve správci front, který vytvořil tuto definici, vloží zprávu do správce front YORK, lokální správce front přeloží název na CLUSQM. Není-li lokální správce front nazván CLUSQM, vloží zprávu do přenosové fronty klastru, která má být přesunuta do adresáře CLUSQM. Také změní záhlaví přenosu tak, aby říkalo CLUSQM místo YORK.

Poznámka: Definice platí pouze pro správce front, který ji vytváří. Chcete-li propagovat alias pro celý klastr, musíte přidat atribut CLUSTER do definice vzdálené fronty. Poté jsou zprávy od jiných správců front, kteří byli určeni pro produkt YORK , odesílány do adresáře CLUSQM.

Změna nebo určení přenosové fronty při odesílání zpráv

Aliasy lze použít pro připojení klastru k systému, který není klastrem. Správci front v klastru ITALY mohou například komunikovat se správcem front s názvem PALERMO, který je mimo klastr. Chcete-li komunikovat, jeden ze správců front v klastru musí fungovat jako brána. Ve správci front brány zadejte příkaz:

```
DEFINE QREMOTE(ROME) RNAME(' ') RQMNAME(PALERMO) XMITQ(X) CLUSTER(ITALY)
```

Příkaz je definicí aliasu správce front. Definuje a inzeruje produkt ROME jako správce front, přes kterého mohou zprávy z libovolného správce front v klastru ITALY více přechodů dosáhnout svého cíle v PALERMO. Zprávy vkládané do fronty otevřené s názvem správce front nastaveným na hodnotu ROME jsou odesílány správci front brány s definicí aliasu správce front. Poté jsou zprávy vloženy do přenosové fronty X a přesunuty kanály mimo klastr do správce front PALERMO.

Volba názvu ROME v tomto příkladu není významná. Hodnoty pro QREMOTE a RQMNAME mohou být stejné.

Určení místa určení při příjmu zpráv

Když správce front obdrží zprávu, extrahuje název cílové fronty a správce front ze záhlaví přenosu. Hledá definici aliasu správce front se stejným názvem jako správce front v záhlaví přenosu. Pokud nějaký nalezne, nahradí hodnotu RQMNAME z definice aliasu správce front názvem správce front v záhlaví přenosu.

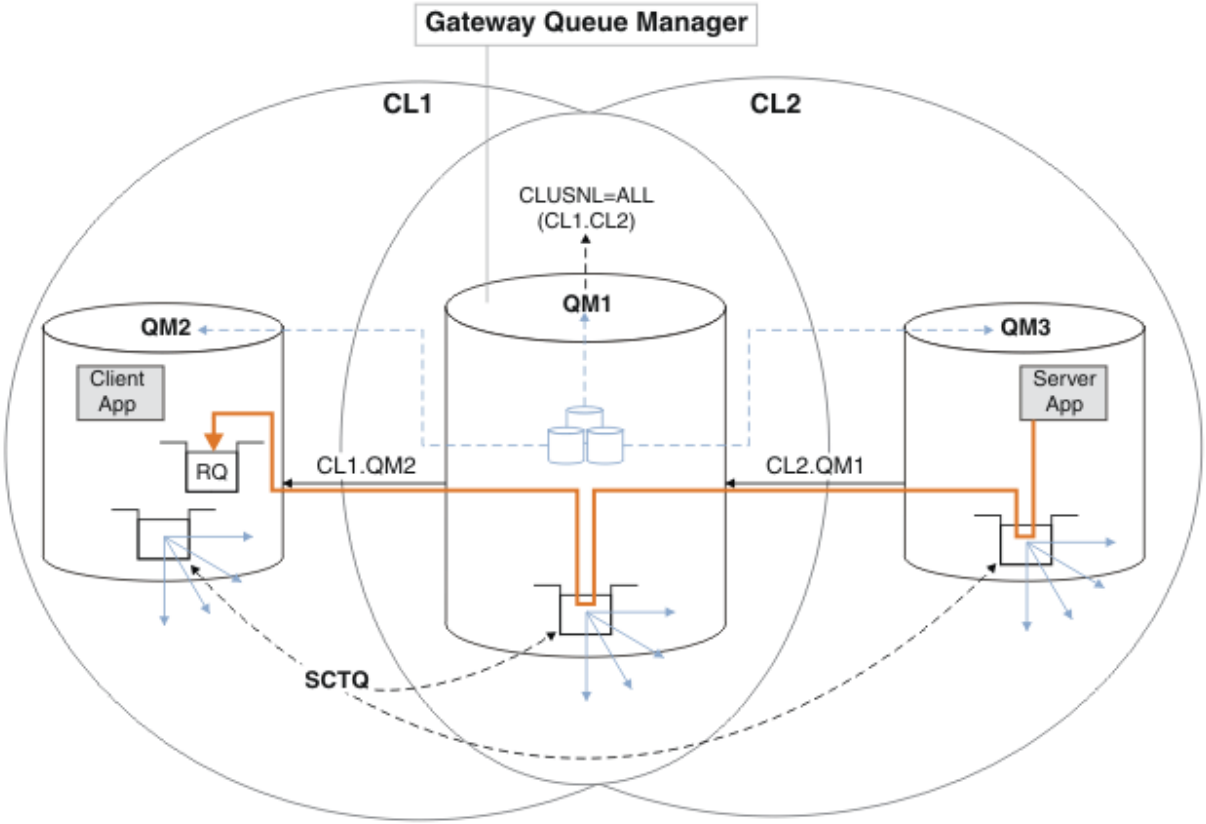
Existují dva důvody pro použití aliasu správce front tímto způsobem:

- Přesměrování zpráv na jiného správce front
- Chcete-li změnit název správce front tak, aby byl stejný jako lokální správce front

Použití aliasů správce front ve správci front brány ke 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 spojuje tyto dva klastry. Není-li fronta definována jako klastrovaná, aby bylo možné provést správné směrování, musí aplikace otevřít frontu s použitím názvu fronty a aliasu správce front v clusteru. Příklad konfigurace viz “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 331, ze kterého je převzat tok zpráv odpovědi znázorněn 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 58. 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 do klastru k vyrovnání zátěže od zpráv přicházejících mimo klastr.

Frontu s názvem EDINBURGH definujete ve více než jednom správci front v klastru. Chcete, aby mechanizmus klastrování vyvážil pracovní zátěž pro zprávy přicházející do této fronty mimo klastr.

Správce front mimo klastr potřebuje přenosovou frontu a odesílací kanál pro jednoho správce front v klastru. Tato fronta se nazývá správce front brány. Chcete-li využít výchozí mechanizmus vyrovnávání pracovní zátěže, musíte použít jedno z následujících pravidel:

- Správce front brány nesmí obsahovat instanci fronty EDINBURGH .
- Správce front brány uvádí CLWLUSEQ(ANY) on ALTER QMGR.

Příklad vyvažování pracovní zátěže mimo klastr viz “Konfigurace vyrovnávání pracovní zátěže mimo klastr” na stránce 372 .

Související pojmy

Aliasy a klastry fronty pro odpovědi
Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Aliasy front a klastry
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr
Nakonfigurujte cestu ke zprávě požadavku/odpovědi ze správce front mimo klastr. Skrytí vnitřních podrobností klastru pomocí správce front brány jako komunikační cesty do klastru a z klastru.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě požadavku/odpovědi z klastru do správce front mimo klastr. Skrýt podrobnosti o způsobu, jakým správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

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.

Aliasy a klastry fronty pro odpovědi

Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Příklad:

- Aplikace ve správci front VENICE odešle zprávu správci front PISA pomocí volání MQPUT . Aplikace poskytuje v deskriptoru zprávy následující informace o frontě pro odpovědi:

```
ReplyToQ='QUEUE'
ReplyToQMgr=''
```

- Aby mohly být odpovědi odeslané do produktu QUEUE přijaty v systému OTHERQ at PISA, vytvořte definici vzdálené fronty v systému VENICE , která se používá jako alias fronty pro odpověď. Alias je účinný pouze v systému, ve kterém byl vytvořen.

```
DEFINE QREMOTE(QUEUE) RNAME(OTHERQ) RQMNAME(PISA)
```

Názvy RQMNAME a QREMOTE mohou být stejné, i když RQMNAME je sám správcem front klastru.

Související pojmy

Aliasy a klastry správce front
Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

Aliasy front a klastry
Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

Související úlohy

Konfigurace požadavku/odpovědi na klastr
Nakonfigurujte cestu ke zprávě požadavku/odpovědi ze správce front mimo klastr. Skrytí vnitřních podrobností klastru pomocí správce front brány jako komunikační cesty do klastru a z klastru.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě požadavku/odpovědi z klastru do správce front mimo klastr. Skrýt podrobnosti o způsobu, jakým správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

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.

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.

Související pojmy

Aliasy a klastry správce front

Aliasy správců front slouží ke skrytí názvů správců front při odesílání zpráv do klastru nebo z klastru a k vyrovnávání pracovní zátěže zpráv odesílaných do klastru.

Aliasy a klastry fronty pro odpovědi
Definice aliasu fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice aliasů front pro odpovědi lze použít s klastry stejně jako v prostředí distribuovaných front.

Související úlohy

Konfigurace požadavku/odpovědi na klastr
Nakonfigurujte cestu ke zprávě požadavku/odpovědi ze správce front mimo klastr. Skrytí vnitřních podrobností klastru pomocí správce front brány jako komunikační cesty do klastru a z klastru.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě požadavku/odpovědi z klastru do správce front mimo klastr. Skrýt podrobnosti o způsobu, jakým správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

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.

Použití klastrů pro správu pracovní zátěže

Definováním více instancí fronty v různých správcích front v klastru můžete rozložit práci obsluhy fronty na více serverů. Existuje několik faktorů, které mohou zabránit tomu, aby byly zprávy v případě selhání znovu zařazeny do fronty pro jiného správce front.

Kromě nastavení klastrů pro omezení administrace systému můžete vytvořit klastry, ve kterých je více než jeden správce front hostitelem instance stejné fronty.

Klastr můžete uspořádat tak, aby v něm byli správci front navzájem klony. Každý správce front může spouštět stejné aplikace a mít lokální definice stejných front. z/OS Například v paralelním prostředí sysplex systému z/OS mohou klonované aplikace přistupovat k datům ve sdílené databázi Db2 nebo v databázi VSAM (Virtual Storage Access Method). Pracovní zátěž můžete rozdělit mezi správce front tak, že budete mít několik instancí aplikace. Každá instance aplikace přijímá zprávy a spouští se nezávisle na ostatních.

Výhody použití klastrů tímto způsobem jsou následující:

- Zvýšená dostupnost front a aplikací.
- Rychlejší propustnost zpráv.
- Rovnoměrnější rozložení pracovní zátěže ve vaší síti.

Každý správce front, který je hostitelem instance konkrétní fronty, může zpracovávat zprávy určené pro tuto frontu a aplikace při odesílání zpráv nepojmenují správce front. Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být zpráva směrována. Vhodné cíle jsou vybrány na základě dostupnosti správce front a fronty a na základě řady atributů specifických pro pracovní zátěž klastru, které jsou přidruženy ke správcům front, frontám a kanálům. Viz Vyvažování pracovní zátěže v klastrech.

z/OS V produktu IBM MQ for z/OSmohou správci front, kteří jsou ve skupinách sdílení front, hostovat fronty klastru jako sdílené fronty. Sdílené fronty klastru jsou k dispozici všem správcům front ve stejné skupině sdílení front. Například v prostředí Klastr s více instancemi stejné frontymohou být jedním nebo oběma správci front QM2 a QM4 sdíleným správcem front. Každá z nich má definici pro frontu Q3. Všichni správci front ve stejné skupině sdílení front jako QM4 mohou číst zprávu vloženou do sdílené fronty Q3. Každá skupina sdílení front může obsahovat až 32 správců front, z nichž každý má přístup ke stejným datům. Sdílení front významně zvyšuje propustnost zpráv.

Další informace o konfiguracích klastrů pro správu pracovní zátěže naleznete v následujících dílčích tématech:

Související pojmy

Porovnání klastrování a distribuovaného řazení do front

Distribuované řazení do front a klastry

Komponenty klastru

Kanály klastru

Co se stane, když je fronta klastru pro MQPUT zakázána

Vyrovnávání pracovní zátěže nastavené v kanálu odesilatele klastru nefunguje.

“Směrování zpráv do klastrů a z klastrů” na stránce 363

Pomocí aliasů front, aliasů správců front a definic vzdálených front můžete připojovat klastry k externím správcům front a dalším klastrům.

Související úlohy

Zápis a kompilace uživatelských procedur pracovní zátěže klastru

“Konfigurace klastru správců front” na stránce 284

Klastry poskytují mechanizmus pro propojení správců front způsobem, který zjednodušuje počáteční konfiguraci i průběžnou správu. Můžete definovat komponenty klastru a vytvářet a spravovat klastry.

“Nastavení nového klastru” na stránce 297

Postupujte podle těchto pokynů, abyste nastavili ukázkový klastr. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosovými frontami. Otestujte práci klastru odesláním zprávy z jednoho správce front do druhého.

“Konfigurace vyrovnávání pracovní zátěže mimo klastr” na stránce 372

Nakonfigurujte cestu ke zprávě ze správce front mimo klastr na libovolnou kopii fronty klastru. Výsledkem je vyrovnávání pracovní zátěže požadavků mimo klastr pro každou instanci fronty klastru.

Související odkazy

Ukázkový program pro monitorování front klastru (AMQSCLM)

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

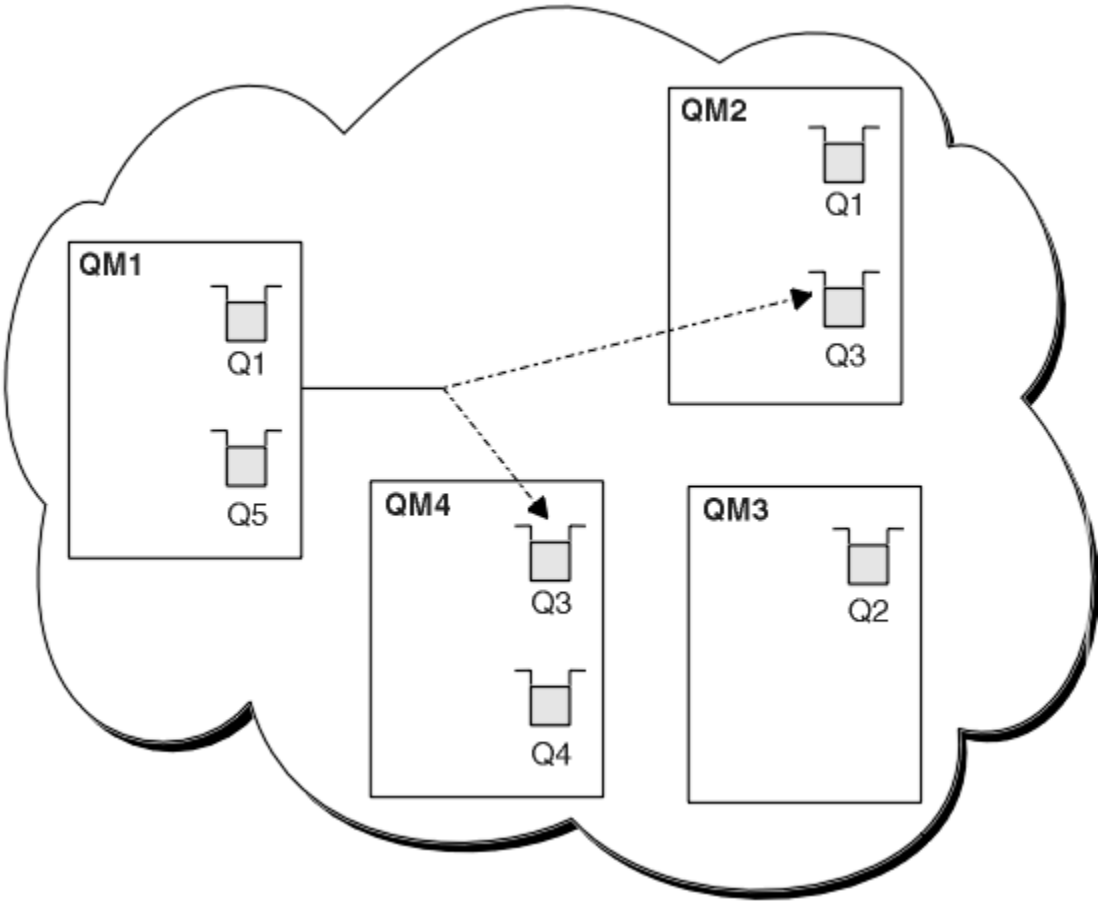
Obrázek 59 na stránce 383 zobrazuje klastr, ve kterém je pro frontu více než jedna definice Q3. Pokud aplikace v adresáři QM1 vloží zprávu do souboru Q3, nemusí nutně vědět, která instance produktu Q3 bude zpracovávat svou zprávu. Pokud je aplikace spuštěna v systému QM2 nebo QM4, , kde jsou lokální instance produktu Q3, otevře se standardně lokální instance produktu Q3 . Nastavením atributu fronty CLWLUSEQ lze s lokální instancí fronty zacházet stejně jako se vzdálenou instancí fronty.

Volba MQOPEN DefBind řídí, zda je vybrán cílový správce front při vydání volání MQOPEN nebo při přenosu zprávy z přenosové fronty.

Nastavíte-li volbu DefBind na hodnotu MQBND_BIND_NOT_FIXED , může být zpráva odeslána do instance fronty, která je k dispozici při přenosu zprávy. Tím se vyhnete následujícím problémům:

- Cílová fronta není k dispozici, když zpráva dorazí do cílového správce front.
- Stav fronty se změnil.
- Zpráva byla vložena s použitím aliasu fronty klastru a ve správci front, kde je definována instance aliasu fronty klastru, neexistuje žádná instance cílové fronty.

Pokud jsou tyto problémy zjištěny v době přenosu, je hledána jiná dostupná instance cílové fronty a zpráva je přesměrována. Pokud nejsou k dispozici žádné instance fronty, zpráva se umístí do fronty nedoručených zpráv.



Obrázek 59. Klastr s více instancemi stejné fronty

Jedním z faktorů, který může zabránit přesměrování zpráv, je přiřazení zpráv k pevnému správci front nebo kanálu pomocí příkazu `MQBND_BIND_ON_OPEN`. Zprávy vázané na `MQOPEN` nejsou nikdy znovu přiděleny k jinému kanálu. Všimněte si také, že k realokaci zpráv dochází pouze v případě, že kanál klastru skutečně selhává. K opětovnému přidělení nedochází, pokud již kanál selhal.

Systém se pokusí přesměrovat zprávu v případě, že správce cílové fronty bude mimo službu. Tím neovlivní integritu zprávy tím, že podstupuje riziko její ztráty nebo vytvořením duplikátu. Pokud se správce front nezdaří a zanechá zprávu v nejistém stavu, nebude tato zpráva přesměrována.

z/OS V systému IBM MQ for z/OSse kanál úplně nezastaví, dokud nebude proces realokace zprávy dokončen. Zastavení kanálu s režimem nastaveným na hodnotu `FORCE` nebo `TERMINATE` proces přeruší, takže pokud tak učiníte, některé zprávy `BIND_NOT_FIXED` již mohly být znovu přiděleny jinému kanálu nebo zprávy mohou být mimo pořadí.

Poznámka: z/OS

1. Před nastavením klastru, který má více instancí stejné fronty, se ujistěte, že vaše zprávy nemají vzájemné závislosti. Například je třeba, aby byla zpracována ve specifické posloupnosti nebo stejným správcem front.
2. Učiňte definice pro různé instance stejné fronty identické. Jinak získáte různé výsledky z různých volání `MQINQ` .

Související pojmy

Programování aplikací a klastry

Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci produktu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Použití dvou sítí v klastru
Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Přidání fronty, která bude fungovat jako záloha
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Omezení počtu použitých kanálů
Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci produktu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v tématu Přidání nového správce front do klastru. Obsahuje tři správce front: LONDON a NEWYORK obě obsahují úplná úložiště, PARIS obsahují dílčí úložiště. Aplikace inventáře je spuštěna v systému v New Yorku a je připojena ke správci front NEWYORK . Aplikace je řízena příchodem zpráv do fronty INVENTQ .
- Chceme přidat instanci produktu INVENTQ , která poskytne další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Informace o této úloze

Chcete-li přidat správce front, který je hostitelem fronty lokálně, postupujte takto.

Postup

1. Změňte správce front PARIS .

   Aby aplikace v Paříži používala databázi INVENTQ v Paříži a aplikaci v New Yorku, musíme informovat správce front. V systému PARIS zadejte následující příkaz:

   ```
   ALTER QMGR CLWLUSEQ(ANY)
   ```

2. Zkontrolujte afinitu zpráv v aplikaci inventáře.

   Než budete pokračovat, ujistěte se, že aplikace inventáře nemá žádné závislosti na posloupnosti zpracování zpráv. Další informace naleznete v tématu Zpracování afinit zpráv.

3. Nainstalujte aplikaci inventáře na systém v Paříži.

4. Definujte frontu klastru INVENTQ.

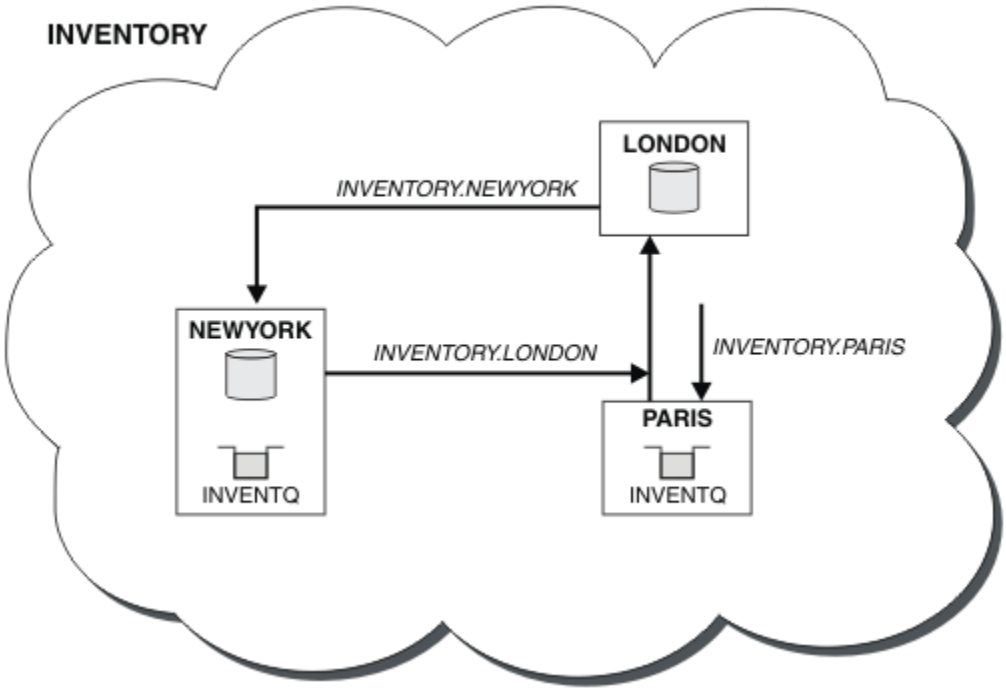
   Hostitelem fronty INVENTQ , jejímž hostitelem je již správce front NEWYORK , je také PARIS. Definujte jej ve správci front PARIS takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte inicializátor kanálu na systému IBM MQ for z/OS. Na všech platformách spusťte program modulu listener ve správci front PARIS. Modul listener naslouchá příchozím síťovým požadavkům a v případě potřeby spustí přijímací kanál klastru.

Výsledky

Obrázek 60 na stránce 385 zobrazuje klastr nastavený touto úlohou.



Obrázek 60. Klastr INVENTORY se třemi správci front

Úprava tohoto klastru byla provedena bez změny správců front NEWYORK nebo LONDON. Úplná úložiště v těchto správcích front jsou automaticky aktualizována o informace, které potřebují k tomu, aby mohli odesílat zprávy na adresu INVENTQ na adrese PARIS.

Jak pokračovat dále

Fronta INVENTQ a aplikace inventáře jsou nyní hostovány na dvou správcích front v klastru. To zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje rozdělit pracovní zátěž mezi dva správce front. Zprávy vkládané do souboru INVENTQ kterýmkoli ze správců front LONDON, NEWYORK, PARIS jsou směrovány střídavě do adresáře PARIS nebo NEWYORK, aby byla pracovní zátěž vyvážená.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

Programování aplikací a klastry

Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána do stejné instance fronty.

Související úlohy

Použití dvou sítí v klastru
Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Přidání fronty, která bude fungovat jako záloha
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Omezení počtu použitých kanálů
Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

Použití dvou sítí v klastru

Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v tématu "Přidání správce front do klastru". Obsahuje tři správce front: LONDON a NEWYORK obě obsahují úplná úložiště, PARIS obsahují dílčí úložiště. Aplikace inventáře je spuštěna v systému v New Yorku a je připojena ke správci front NEWYORK . Aplikace je řízena příchodem zpráv do fronty INVENTQ .
- V produktu TOKYO se přidává nové úložiště, kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Informace o této úloze

Chcete-li použít dvě sítě v klastru, postupujte takto.

Postup

1. Nejprve rozhodněte, na které úplné úložiště TOKYO odkazuje.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Vytváří vlastní dílčí úložiště. Úložiště, které zvolíte, nemá žádný zvláštní význam. V tomto příkladu je vybrána volba NEWYORK . Jakmile se nový správce front připojí ke klastru, komunikuje s oběma úložišti.
2. Definujte kanály CLUSRCVR .

   Každý správce front v klastru musí definovat příjemce klastru, na kterém může přijímat zprávy. Tento správce front musí být schopen komunikovat v 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. Definovat kanál CLUSSDR ve správci front TOKYO.

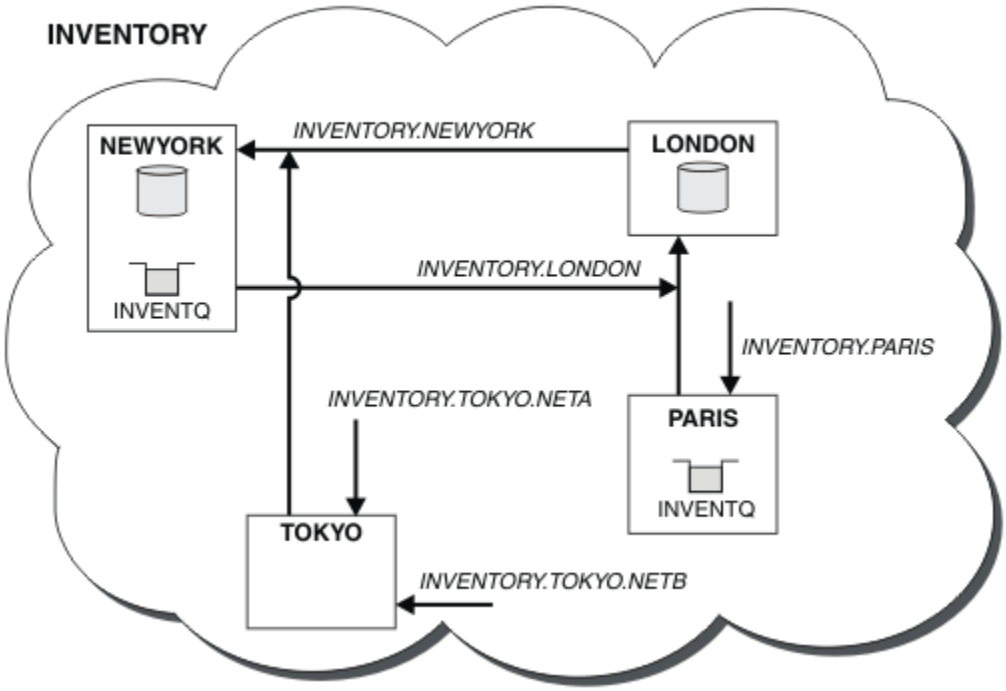
   Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK, takže TOKYO potřebuje následující definici:

   ```
   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 inicializátor kanálu na systému IBM MQ for z/OS. Na všech platformách spusťte program modulu listener ve správci front PARIS. Program listener naslouchá příchozím síťovým požadavkům a v případě potřeby spustí přijímací kanál klastru.

Výsledky

Obrázek 61 na stránce 387 zobrazuje klastr nastavený touto úlohou.



Obrázek 61. Klastr INVENTORY se čtyřmi správci front

Po vytvoření pouze tří definic jsme přidali správce front TOKYO do klastru se dvěma různými síťovými cestami, které jsou k dispozici.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

Programování aplikací a klastry
Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci produktu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Přidání fronty, která bude fungovat jako záloha
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Omezení počtu použitých kanálů
Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

“Přidání správce front do klastru” na stránce 308
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle těchto pokynů.
Zprávy do front 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 nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Použití dvou sítí v klastru” na stránce 386. Obsahuje čtyři správce front; LONDON a NEWYORK oba zadržují úplná úložiště; PARIS a TOKYO zadržují dílčí úložiště. Aplikace inventáře je spuštěna v systému v New Yorku a je připojena ke správci front NEWYORK. Správce front TOKYO má dvě různé sítě, ve kterých může komunikovat.
- Chcete nastavit jednu ze sítí jako primární síť a druhou síť jako záložní síť. Pokud se vyskytne problém s primární sítí, plánujete použít záložní síť.

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 určit, že kanál sítě A je primárním kanálem a kanál sítě B je sekundárním kanálem, 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 pro klastr, že máte primární síť a sekundární síť. Správci front v klastru, kteří používají tyto kanály, automaticky používají primární síť, kdykoli je k dispozici. Správce front provede překonání selhání pro použití sekundární sítě v případě, že primární síť není k dispozici.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

Programování aplikací a klastry
Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci produktu `INVENTQ` , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Použití dvou sítí v klastru
Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu `TOKYO` , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Přidání fronty, která bude fungovat jako záloha
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Omezení počtu použitých kanálů
Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

Přidání fronty, která bude fungovat jako záloha

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr `INVENTORY` byl nastaven podle popisu v části “Přidání správce front do klastru” na stránce 308. Obsahuje tři správce front: `LONDON` a `NEWYORK` obě obsahují úplná úložiště, `PARIS` obsahují dílčí úložiště. Aplikace inventáře je spuštěna v systému v New Yorku a je připojena ke správci front `NEWYORK` . Aplikace je řízena příchodem zpráv do fronty `INVENTQ` .
- V Chicagu je zřízen nový obchod, který poskytuje zálohu pro systém inventáře, který nyní běží v New Yorku. Chicagský systém se používá pouze v případě, že je problém se systémem New York.

Informace o této úloze

Chcete-li přidat frontu, která bude fungovat jako záloha, postupujte takto.

Postup

1. Nejprve rozhodněte, na které úplné úložiště CHICAGO odkazuje.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Vytváří vlastní dílčí úložiště. Nemá žádný zvláštní význam, které úložiště vyberete pro konkrétního správce front. V tomto příkladu je vybrána volba NEWYORK . Jakmile se nový správce front připojí 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 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.

   INVENTQ , jehož hostitelem je již správce front NEWYORK , je hlavní instancí fronty.

   ```
   ALTER QLOCAL(INVENTQ) CLWLPRTY(2)
   ```
5. Zkontrolujte afinitu zpráv v aplikaci inventáře.

   Než budete pokračovat, ujistěte se, že aplikace inventáře nemá žádné závislosti na posloupnosti zpracování zpráv.
6. Nainstalujte aplikaci inventáře na systém v adresáři CHICAGO.
7. Definovat frontu záložního klastru INVENTQ

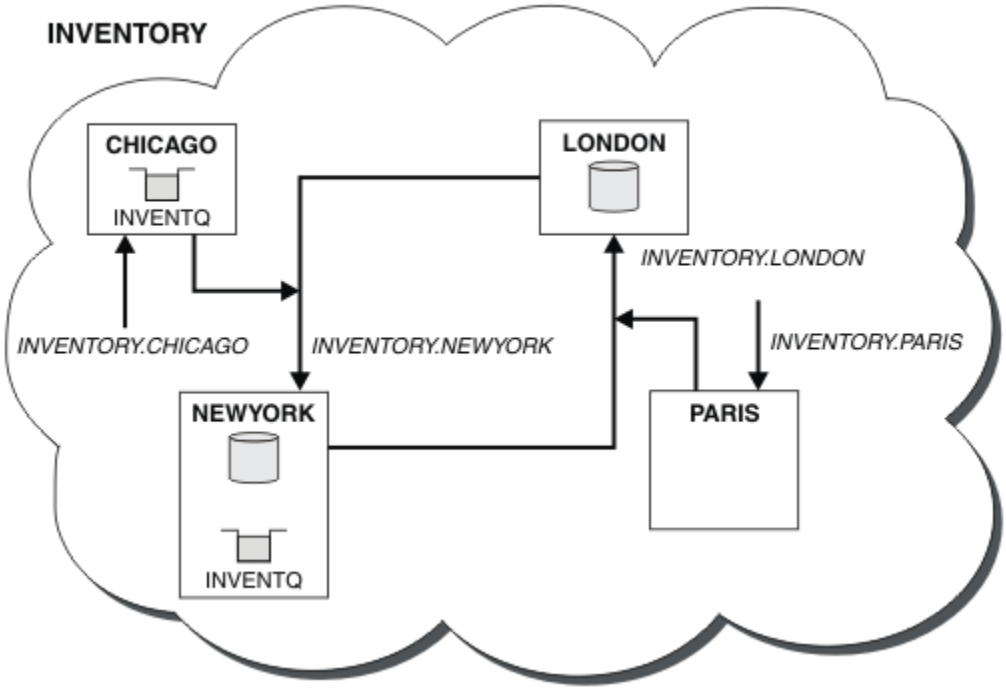
   INVENTQ , jehož hostitelem je již správce front NEWYORK , má být také hostován jako záloha produktem CHICAGO. Definujte jej ve správci front CHICAGO takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) CLWLPRTY(1)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte inicializátor kanálu na systému IBM MQ for z/OS. Na všech platformách spusťte program modulu listener ve správci front CHICAGO. Program listener naslouchá příchozím síťovým požadavkům a v případě potřeby spustí přijímací kanál klastru.

Výsledky

Obrázek 62 na stránce 391 zobrazuje klastr nastavený touto úlohou.



Obrázek 62. Klastr INVENTORY se čtyřmi správci front

Fronta INVENTQ a aplikace inventáře jsou nyní hostovány na dvou správcích front v klastru. Správce front CHICAGO je záloha. Zprávy vkládané do souboru INVENTQ jsou směrovány do adresáře NEWYORK , pokud nejsou k dispozici při jejich odesílání do adresáře CHICAGO.

Poznámka:

Dostupnost vzdáleného správce front je založena na stavu kanálu pro daného správce front. Při spuštění kanálů se jejich stav několikrát změní, přičemž některé ze stavů jsou méně vhodnější než algoritmus správy pracovní zátěže klastru. V praxi to znamená, že lze vybrat cíle s nižší prioritou (záložní), zatímco se začínají kanály s cíli s vyšší prioritou (primární).

Potřebujete-li se ujistit, že do cíle zálohování nepřejdou žádné zprávy, nepoužívejte příkaz CLWLPRTY. Zvažte použití oddělených front nebo CLWLRANK s ručním přepínáním z primárního k zálohování.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

Programování aplikací a klastry
Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci produktu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Použití dvou sítí v klastru
Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Omezení počtu použitých kanálů
Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

Omezení počtu použitých kanálů

Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Aplikace pro kontrolu cen má být instalována v různých správcích front. Chcete-li zachovat počet kanálů používaných na nízký počet, počet aktivních kanálů, které jsou spuštěny na každém serveru, je omezen. Aplikace je řízena příchodem zpráv do fronty PRICEQ .
- Čtyři správci front serveru jsou hostiteli aplikace pro kontrolu cen. Dva správci front dotazů odesílají do produktu PRICEQ zprávy s dotazem na cenu. Další dva správci front jsou nakonfigurováni jako úplná úložiště.

Informace o této úloze

Chcete-li omezit počet použitých kanálů, postupujte takto.

Postup

1. Vyberte dvě úplná úložiště.

   Vyberte dva správce front, kteří mají být úplnými úložišti pro váš klastr pro kontrolu cen. Nazývají se REPOS1 a REPOS2.

   Spusťte následující příkaz:

   ```
   ALTER QMGR REPOS(PRICECHECK)
   ```
2. Definujte kanál CLUSRCVR pro každého správce front.

   U každého správce front v klastru definujte přijímací kanál klastru a odesílací kanál klastru. Nezáleží na tom, který je definován 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 pro každého správce front definici CLUSSDR , aby bylo možné tohoto správce front propojit 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 pro kontrolu cen.
5. Definujte frontu PRICEQ ve všech správcích front serveru.

   Zadejte následující příkaz pro každý z nich:

   ```
   DEFINE QLOCAL(PRICEQ) CLUSTER(PRICECHECK)
   ```

6. Omezit počet kanálů používaných dotazy

   Ve správcích front dotazů omezujeme počet použitých aktivních kanálů zadáním následujících příkazů pro jednotlivé kanály:

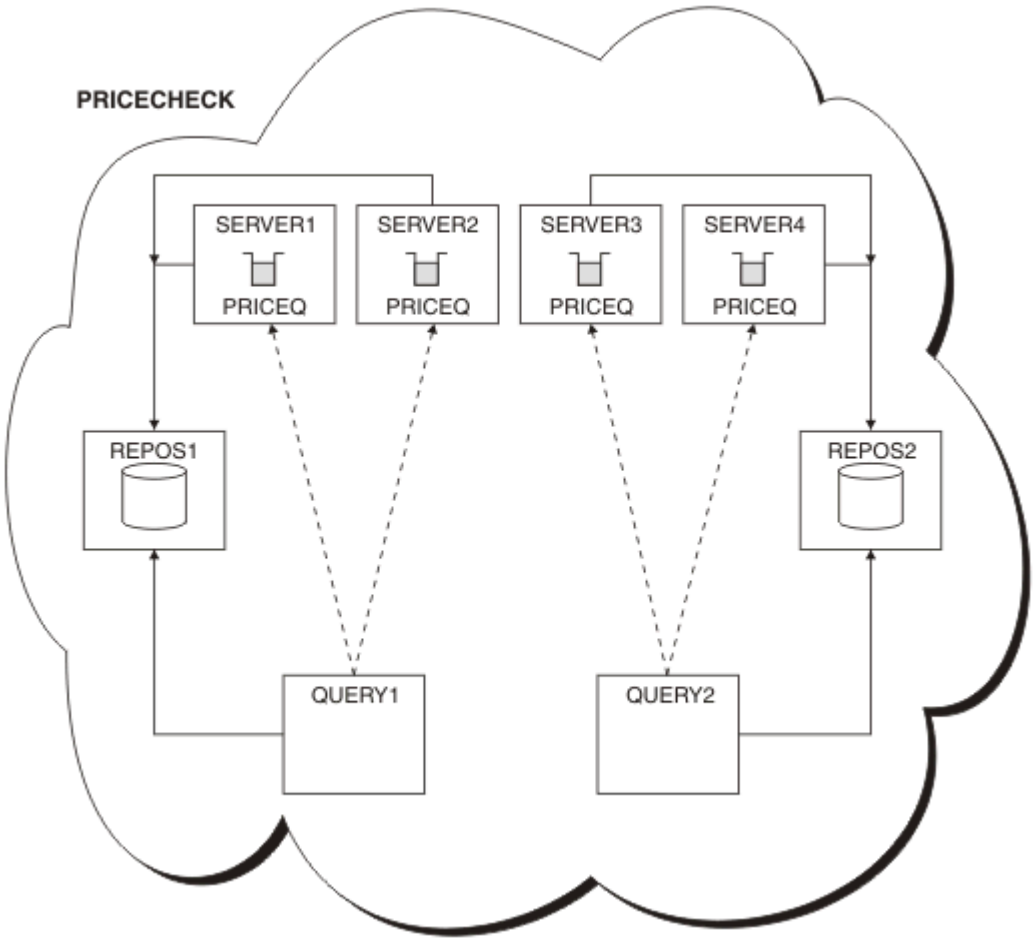
   ```
   ALTER QMGR CLWLMRUC(2)
   ```

7. Pokud jste tak dosud neučinili, spusťte inicializátor kanálu na systému IBM MQ for z/OS. Na všech platformách spusťte program modulu listener.

   Program listener naslouchá příchozím síťovým požadavkům a v případě potřeby spustí přijímací kanál klastru.

Výsledky

Obrázek 63 na stránce 393 zobrazuje klastr nastavený touto úlohou.



Obrázek 63. Klastr PRICECHECK se čtyřmi správci front serveru, dvěma úložišti a dvěma správci front dotazů.

Ačkoli jsou v klastru PRICECHECK k dispozici čtyři instance fronty PRICEQ , každý dotazující se správce front používá pouze dvě z nich. Například správce front QUERY1 má aktivní kanály pouze pro správce front SERVER1 a SERVER2 . Pokud se SERVER1 stane nedostupným, začne správce front QUERY1 používat jiného správce front, například SERVER3.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

Programování aplikací a klastry
Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci produktu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Použití dvou sítí v klastru
Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Přidání fronty, která bude fungovat jako záloha
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

Než začnete

Poznámka: Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Přidání správce front do klastru” na stránce 308. Obsahuje tři správce front: LONDON a NEWYORK oba zadržují úplná úložiště, PARIS zadržuje dílčí úložiště a vkládá zprávy z INVENTQ. Aplikace inventáře je spuštěna v systému v New Yorku připojeném ke správci front NEWYORK . Aplikace je řízena příchodem zpráv do fronty INVENTQ .
- V Los Angeles se zřizují nové prodejny. Chcete-li poskytnout další kapacitu, chcete spustit inventární systém v Los Angeles, stejně jako v New Yorku. Nový správce front může zpracovat dvakrát více zpráv než New York.

Informace o této úloze

Chcete-li přidat výkonnějšího správce front, který je hostitelem fronty, postupujte takto.

Postup

1. Nejprve rozhodněte, na které úplné úložiště LOSANGELES odkazuje.
2. Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Vytváří vlastní dílčí úložiště. Úložiště, které zvolíte, nemá žádný zvláštní význam. V tomto příkladu je vybrána volba NEWYORK . Jakmile se nový správce front připojí 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 přijímací kanál klastru, na 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 inzeruje dostupnost správce front pro příjem zpráv od jiných správců front v klastru INVENTORY. Nastavení parametru CLWLWGHT na hodnotu dvě zajistí, že správce front Los Angeles obdrží dvakrát více zpráv inventáře než New York (když je kanál pro NEWYORK nastaven na hodnotu jedna).
4. Změňte kanál CLUSRCVR ve správci front NEWYORK.

   Ujistěte se, že správce front Los Angeles obdrží dvakrát více zpráv inventáře než New York. Změňte definici přijímacího kanálu klastru.

   ```
   ALTER CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) CLWLWGHT(1)
   ```
5. Zkontrolujte afinitu zpráv v aplikaci inventáře.

   Než budete pokračovat, ujistěte se, že aplikace inventáře nemá žádné závislosti na posloupnosti zpracování zpráv.
6. Nainstalujte aplikaci inventáře na systém v Los Angeles
7. Definujte frontu klastru INVENTQ.

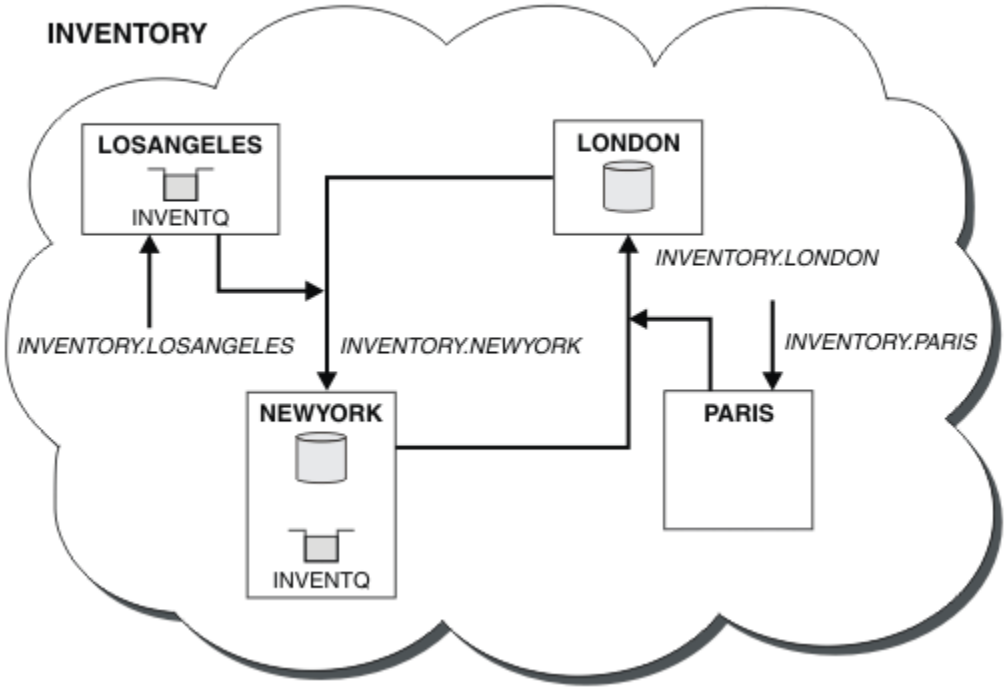
   Hostitelem fronty INVENTQ , jejímž hostitelem je již správce front NEWYORK , bude také LOSANGELES. Definujte jej ve správci front LOSANGELES takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte inicializátor kanálu na systému IBM MQ for z/OS. Na všech platformách spusťte program modulu listener ve správci front LOSANGELES. Program listener naslouchá příchozím síťovým požadavkům a v případě potřeby spustí přijímací kanál klastru.

Výsledky

“Přidání výkonnějšího správce front, který je hostitelem fronty” na stránce 394 zobrazuje klastr nastavený touto úlohou.



Obrázek 64. Klastr INVENTORY se čtyřmi správci front

Tato úprava klastru byla provedena bez nutnosti změny správců front LONDON a PARIS. Úložiště v těchto správcích front jsou automaticky aktualizována informacemi, které potřebují k odesílání zpráv do INVENTQ na adrese LOSANGELES.

Jak pokračovat dále

Fronta INVENTQ a aplikace inventáře jsou hostovány ve dvou správcích front v klastru. Konfigurace zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje distribuci pracovní zátěže mezi dvěma správci front. Zprávy vkládané do souboru INVENTQ buď LOSANGELES , nebo NEWYORK jsou zpracovány instancí v lokálním správci front, kdykoli je to možné. Zprávy vkládané pomocí LONDON nebo PARIS jsou směrovány do LOSANGELES nebo NEWYORK, přičemž dvakrát tolik zpráv je odesíláno do LOSANGELES.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

Programování aplikací a klastry
Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci produktu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Použití dvou sítí v klastru
Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Přidání fronty, která bude fungovat jako záloha
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Omezení počtu použitých kanálů
Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Programování aplikací a klastry

Nemusíte provádět žádné programovací změny, abyste využili více instancí stejné fronty. Některé programy však nefungují správně, pokud není posloupnost zpráv odeslána 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 nastavíte klastry, které mají více instancí stejné fronty, neexistují žádné specifické aspekty programování aplikací. Chcete-li však využívat výhod aspektů správy pracovní zátěže klastrování, budete možná muset upravit své aplikace. Pokud nastavíte síť, ve které existuje více definic stejné fronty, zkontrolujte, zda aplikace nepoužívají afinity zpráv.

Předpokládejme například, že máte dvě aplikace, které spoléhají na řadu zpráv, které mezi nimi proudí ve formě otázek a odpovědí. Pravděpodobně budete chtít, aby se odpovědi vrátily ke stejnému správci front, který odeslal otázku. Je důležité, aby rutina správy pracovní zátěže neodesílala zprávy žádnému správci front, který je hostitelem kopie fronty odpovědí.

Můžete mít aplikace, které vyžadují, aby byly zprávy zpracovány postupně (například aplikace replikace databáze, která odesílá dávky zpráv, které musí být načteny v posloupnosti). Použití segmentovaných zpráv může také způsobit problém s afinitou.

Otevření lokální nebo vzdálené verze cílové fronty

Mějte na paměti, jak správce front vybírá, zda používá lokální nebo vzdálenou verzi cílové fronty.

1. Správce front otevře lokální verzi cílové fronty pro čtení zpráv nebo pro nastavení atributů fronty.
2. Správce front otevře libovolnou instanci cílové fronty pro zápis zpráv, pokud je splněna alespoň jedna z následujících podmínek:
   - Lokální verze cílové fronty neexistuje.
   - Správce front uvádí `CLWLUSEQ(ANY)` on `ALTER QMGR`.
   - Fronta ve správci front uvádí `CLWLUSEQ(ANY)`.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány do různých instancí fronty. Můžete vynutit zprávu pro specifickou instanci fronty a můžete zvolit odeslání posloupnosti zpráv jednomu ze správců front.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci produktu `INVENTQ` , abyste poskytli další kapacitu pro spuštění systému aplikace inventáře v Paříži a New Yorku.

Použití dvou sítí v klastru
Postupujte podle těchto pokynů, chcete-li přidat nové úložiště v produktu `TOKYO` , kde jsou dvě různé sítě. Oba musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li nastavit jednu síť jako primární síť a jinou síť jako záložní síť. Je-li problém s primární sítí, použijte záložní síť.

Přidání fronty, která bude fungovat jako záloha

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém inventáře, který je nyní spuštěn v New Yorku. Chicagský systém se používá pouze v případě, že existuje problém se systémem New York.

Omezení počtu použitých kanálů
Při instalaci aplikace pro kontrolu cen v různých správcích front omezte počet aktivních kanálů, které jsou na jednotlivých serverech spuštěny, podle těchto pokynů.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, abyste poskytli dodatečnou kapacitu spuštěním inventárního systému v Los Angeles, stejně jako v New Yorku, kde Los Angeles může zpracovat dvojnásobný počet zpráv jako New York.

Zpracování afinit zpráv
Spřízněnosti zpráv jsou zřídkakdy součástí dobrého programovacího návrhu. Chcete-li plně používat klastrování, musíte odebrat afinity zpráv. Pokud nemůžete odebrat afinity zpráv, můžete vynutit doručení souvisejících zpráv pomocí stejného kanálu a stejného správce front.

Máte-li aplikace se spřízněností zpráv, odeberte spřízněnosti před tím, než začnete používat klastry.

Odebrání afinit zpráv zlepšuje dostupnost aplikací. Aplikace odešle dávku zpráv, které mají afinitu zpráv, do správce front. Správce front selže po přijetí pouze části dávky. Odesílající správce front musí čekat na zotavení a zpracování neúplné dávky zpráv, než bude moci odeslat další zprávy.

Odebrání afinit zpráv také zlepšuje rozšiřitelnost aplikací. Dávka zpráv s afinitami může uzamknout prostředky v cílovém správci front při čekání na následné zprávy. Tyto prostředky mohou zůstat uzamčené po dlouhou dobu, což brání ostatním aplikacím v práci.

Afinity zpráv navíc brání rutinám správy pracovní zátěže klastru v nejlepší volbě správce front.

Chcete-li odstranit afinity, zvažte následující možnosti:

- Přenášení informací o stavu ve zprávách
- Udržování informací o stavu v energeticky nezávislé paměti přístupné pro libovolného správce front, například v databázi Db2
- Replikace dat jen pro čtení tak, aby byla přístupná pro více než jednoho správce front

Pokud není vhodné upravit aplikace tak, aby odebírovaly afinity zpráv, existuje řada možných řešení problému.

Pojmenujte konkrétní místo určení ve volání `MQOPEN` .

Při každém volání produktu `MQOPEN` zadejte název vzdálené fronty a název správce front a všechny zprávy vkládané do fronty s použitím daného popisovače objektu přejdou na stejného správce front, kterým může být lokální správce front.

Určení názvu vzdálené fronty a názvu správce front pro každé volání `MQOPEN` má nevýhody:

- Neprovádí se žádné vyrovnávání pracovní zátěže. Nevyužíváte výhod vyrovnávání pracovní zátěže klastru.
- Pokud je cílový správce front vzdálený a existuje pro něj více než jeden kanál, zprávy mohou mít různé trasy a posloupnost zpráv stále není zachována.
- Pokud má váš správce front definici pro přenosovou frontu se stejným názvem jako cílový správce front, zprávy budou v této přenosové frontě namísto v přenosové frontě klastru.

Vrátit název správce front v poli správce front pro odpověď

Povolit správci front, který obdrží první zprávu v dávce, vrátit její název v odpovědi. Provádí to pomocí pole `ReplyToQMgr` deskriptoru zprávy. Správce front na odesílajícím konci pak může extrahovat název správce front pro odpověď a zadat jej pro všechny následné zprávy.

Použití informací `ReplyToQMgr` z odezvy má nevýhody:

- Požadující správce front musí čekat na odpověď na svou první zprávu.

- Chcete-li vyhledat a použít informace ReplyToQMgr před odesláním následných zpráv, musíte napsat další kód.
- Pokud existuje více než jedna trasa ke správci front, nemusí být posloupnost zpráv zachována.

Nastavte volbu MQOO_BIND_ON_OPEN ve volání MQOPEN .

Vynuťte vložení všech zpráv do stejného místa určení pomocí volby MQOO_BIND_ON_OPEN ve volání MQOPEN . Buď MQOO_BIND_ON_OPEN , nebo MQOO_BIND_ON_GROUP musí být zadáno při použití skupin zpráv s klastry, aby se zajistilo, že všechny zprávy ve skupině budou zpracovány ve stejném místě určení.

Otevřením fronty a uvedením parametru MQOO_BIND_ON_OPENvynutíte, aby všechny zprávy odeslané do této fronty byly odeslány do stejné instance fronty. Produkt MQOO_BIND_ON_OPEN sváže všechny zprávy se stejným správcem front a také se stejnou přenosovou cestou. Pokud například existuje přenosová cesta IP a přenosová cesta NetBIOS ke stejnému cíli, jedna z nich je vybrána při otevření fronty a tato volba je uznána pro všechny zprávy vkládané do stejné fronty pomocí získaného popisovače objektu.

Zadáním parametru MQOO_BIND_ON_OPEN vynutíte směrování všech zpráv do stejného místa určení. Proto nejsou narušeny aplikace se spřízněností zpráv. Není-li místo určení k dispozici, zůstanou zprávy v přenosové frontě, dokud nebudou znovu k dispozici.

Parametr MQOO_BIND_ON_OPEN se použije také v případě, že je při otevření fronty zadán název správce front v deskriptoru objektu. K uvedenému správci front může existovat více než jedna trasa. Může například existovat více síťových cest nebo jiný správce front mohl definovat alias. Zadáte-li MQOO_BIND_ON_OPEN, bude při otevření fronty vybrána přenosová cesta.

Poznámka: Jedná se o doporučenou techniku. Nefunguje však v konfiguraci s více přechody, ve které správce front inzeruje alias pro frontu klastru. Nepomáhá ani v situacích, kdy aplikace používají různé fronty ve stejném správci front pro různé skupiny zpráv.

Alternativou k zadání parametru MQOO_BIND_ON_OPEN ve volání MQOPEN je úprava definic front. V definicích front zadejte DEFBIND(OPEN)a povolte volbu DefBind ve volání MQOPEN na výchozí hodnotu MQOO_BIND_AS_Q_DEF.

Nastavte volbu MQOO_BIND_ON_GROUP ve volání MQOPEN .

Vynuťte vložení všech zpráv ve skupině do stejného místa určení pomocí volby MQOO_BIND_ON_GROUP volání MQOPEN . Buď MQOO_BIND_ON_OPEN , nebo MQOO_BIND_ON_GROUP musí být zadáno při použití skupin zpráv s klastry, aby se zajistilo, že všechny zprávy ve skupině budou zpracovány ve stejném místě určení.

Otevřením fronty a uvedením MQOO_BIND_ON_GROUPvynutíte, aby všechny zprávy ve skupině, které jsou odeslány do této fronty, byly odeslány do stejné instance fronty. Produkt MQOO_BIND_ON_GROUP sváže všechny zprávy ve skupině se stejným správcem front a také se stejnou přenosovou cestou. Pokud například existuje přenosová cesta IP a přenosová cesta NetBIOS ke stejnému cíli, jedna z nich je vybrána při otevření fronty a tato volba je uznána pro všechny zprávy ve skupině vkládané do stejné fronty pomocí získaného popisovače objektu.

Zadáním MQOO_BIND_ON_GROUP vynutíte, aby všechny zprávy ve skupině byly směrovány do stejného místa určení. Proto nejsou narušeny aplikace se spřízněností zpráv. Není-li místo určení k dispozici, zůstanou zprávy v přenosové frontě, dokud nebudou znovu k dispozici.

Parametr MQOO_BIND_ON_GROUP se použije také v případě, že je při otevření fronty zadán název správce front v deskriptoru objektu. K uvedenému správci front může existovat více než jedna trasa. Může například existovat více síťových cest nebo jiný správce front mohl definovat alias. Zadáte-li MQOO_BIND_ON_GROUP, bude při otevření fronty vybrána přenosová cesta.

Aby byl příkaz MQOO_BIND_ON_GROUP účinný, musíte do příkazu MQPUT zahrnout volbu vložení MQPMO_LOGICAL_ORDER . Parametr **GroupId** v deskriptoru MQMD zprávy můžete nastavit na hodnotu MQGI_NONEa následující příznaky zprávy musíte zahrnout do pole MQMD **MsgFlags** zpráv:

- Poslední zpráva ve skupině: MQMF_LAST_MSG_IN_GROUP
- Všechny ostatní zprávy ve skupině: MQMF_MSG_IN_GROUP

Je-li zadána hodnota MQOO_BIND_ON_GROUP , ale zprávy nejsou seskupeny, je chování ekvivalentní hodnotě MQOO_BIND_NOT_FIXED.

Poznámka: Jedná se o doporučenou techniku pro zajištění toho, aby zprávy ve skupině byly odesílány do stejného místa určení. Nefunguje však v konfiguraci s více přechody, ve které správce front inzeruje alias pro frontu klastru.

Alternativou k zadání parametru MQOO_BIND_ON_GROUP ve volání MQOPEN je úprava definic front. V definicích front zadejte DEFBIND(GROUP) a povolte volbu DefBind ve volání MQOPEN na výchozí hodnotu MQOO_BIND_AS_Q_DEF.

Napsat přizpůsobený uživatelský program pracovní zátěže klastru

Namísto úpravy aplikací můžete problém se spřízněností zpráv obejít napsáním uživatelského programu pracovní zátěže klastru. Napsání uživatelského programu pracovní zátěže klastru není snadné a není doporučeným řešením. Program by musel být navržen tak, aby rozpoznal afinitu kontrolou obsahu zpráv. Po rozpoznání afinity bude muset program vynutit, aby obslužný program správy pracovní zátěže směroval všechny související zprávy do stejného správce front.

Multi Konfigurace jednotného klastru

Jednotné klastry umožňují navrhovat aplikace pro škálování a dostupnost a mohou se připojovat k libovolným správcům front v rámci tohoto jednotného klastru.

Než začnete

Úvod do klastrování viz Klastry. Úvod do jednotných klastrů viz “O jednotných klastrech” na stránce 400.

Informace o této úloze

Jednotné klastry používají klastrování produktu IBM MQ pro komunikaci mezi správci front a vyrovnávání pracovní zátěže mezi frontami. Liší se však od typických klastrů IBM MQ následujícími způsoby:

- Uniformní klastry mají obvykle menší počet správců front v klastru. Neměli byste vytvářet jednotný klastr s více než 10 správci front.
- Každý člen klastru má téměř identickou konfiguraci.
- Klastr je obvykle používán jednou aplikací nebo skupinou souvisejících aplikací.
- Počet instancí aplikace, které se připojují ke klastru, by měl být větší nebo roven počtu správců front.

Můžete zjednodušit vytvoření jednotného klastru a následně zachovat identickou konfiguraci mezi členy jednotného klastru pomocí automatické konfigurace a podpory automatického klastrování.

Procedura

- Další informace o uniformách klastrů
- Vytvořit uniformní klastr
- Vytvořit uniformní klastr
- Pozastavit správce front z uniformního klastru

Multi O jednotných klastrech

Cílem jednotné implementace klastru je, aby aplikace mohly být navrženy pro škálování a dostupnost a aby se mohly připojovat k libovolným správcům front v rámci uniformního klastru. Tím se odebere jakákoli závislost na specifickém správci front, což povede k lepší dostupnosti a vyrovnávání pracovní zátěže provozu systému zpráv. z/OS Uniformní klastry nejsou k dispozici v systému IBM MQ for z/OS; skupiny sdílení front poskytují mnoho schopností uniformního klastru.

Jednotné klastry jsou specifickým vzorem klastru IBM MQ , který poskytuje malou kolekci správců front s vysokou dostupností a horizontálním měřítkem. Tito správci front jsou nakonfigurováni téměř identicky, takže s nimi může aplikace pracovat jako s jedinou skupinou. To usnadňuje zajištění používání jednotlivých správců front v klastru tím, že se automaticky zajistí rovnoměrné rozložení instancí aplikací mezi správce front.

Uniformní klastry odebírají některé ruční kroky, které musí administrátor provést, aby vytvořil a spravoval skupinu nezávislých, vzájemně propojených správců front. Přesouvají logiku připojení klienta z klienta do správce front, kde mohou informace o úrovních aktivity aplikace informovat klienty o tom, ke kterým správcům front se mají připojit.

Můžete zjednodušit počáteční vytvoření jednotného klastru a následně zachovat identickou konfiguraci mezi členy jednotného klastru pomocí automatické konfigurace a podpory automatického klastrování. Při použití této schopnosti jeden konfigurační soubor popisuje klastr a druhý představuje konfiguraci MQSC, která má být použita pro všechny správce front v jednotném klastru. Při každém restartování správce front se konfigurace znovu použije a klastr se automaticky vytvoří. Další podrobnosti o použití této funkce viz “Vytvoření jednotného klastru” na stránce 414 .

Chcete-li plně využít výhod jednotného klastru, každá aplikace by měla být také škálována na více odpovídajících instancí, nejlépe s alespoň tolika instancemi, kolik existuje správců front, ne-li více.

Klastr IBM MQ libovolné velikosti nabízí více funkcí:

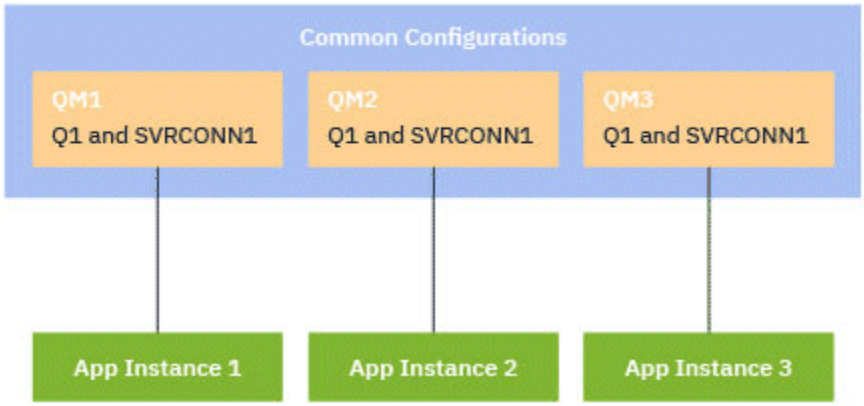
- Adresář všech klastrových prostředků, zjistitelný libovolným členem v klastru
- Automatické vytváření kanálů a konektivita
- Vodorovné škálování ve více odpovídajících frontách s použitím vyrovnávání pracovní zátěže zpráv.
- Dynamické směrování zpráv na základě dostupnosti

Jednotné klastry používají klastrování produktu IBM MQ pro komunikaci mezi správci front a vyrovnávání pracovní zátěže mezi frontami. Liší se však od typických klastrů IBM MQ následujícími způsoby:

- Uniformní klastry mají obvykle menší počet správců front v klastru. Neměli byste vytvářet jednotný klastr s více než 10 správci front.
- Každý člen klastru má téměř identickou konfiguraci.
- Klastr je obvykle používán jednou aplikací nebo skupinou souvisejících aplikací.
- Počet instancí aplikace, které se připojují ke klastru, by měl být větší nebo roven počtu správců front.

V jednotném vzoru klastru nabízejí všichni správci front v klastru stejné služby systému zpráv. Můžete například nakonfigurovat všechny členy klastru tak, aby měli definovány stejné lokální fronty, a umožnit klientským aplikacím připojit se k libovolnému členovi klastru. Můžete mít také definovány stejné kanály připojení serveru a pravděpodobně stejné záznamy oprávnění, pravidla ověřování kanálu atd. Členové klastru však mohou mít stále určité rozdíly v objektech a konfiguraci. Některé aplikace mohou například vytvářet dočasné dynamické fronty v době, kdy jsou připojeny ke správci front. Také některé aktualizace konfigurace mohou být během určitého časového období v rámci členů provedeny; například nové nebo aktualizované certifikáty. Stejně jako u běžných klastrů IBM MQ budou dva správci front vyžadovat další konfiguraci, aby z nich učinili správce front s úplným úložištěm.

Následující diagram ukazuje, že správci front mají podobné konfigurace. Definují stejnou frontu s názvem Q1 a stejný kanál připojení serveru SVRCONN1.



Mějte na paměti, že v případě více správců front s identickými názvy kanálů připojení serveru pro práci s jednou tabulkou CCDT (Client-Channel Definition Table) je nutné použít aktualizovaný formát CCDT zavedený v souboru IBM MQ 9.1.2. Viz téma “Konfigurace formátu JSON CCDT” na stránce 44.

Názvy aplikací a instance aplikací

Název aplikace se zobrazí jako atribut APPLTAG příkazu **DISPLAY CONN(*) TYPE CONN** . V produktu IBM MQ 9.1.2dochází ke změně způsobu nastavení názvu aplikace.

Instance aplikace je sada úzce souvisejících připojení, která poskytují jednu *jednotku provedení* pro tuto aplikaci. Obvykle se jedná o jeden proces operačního systému, který může mít několik podprocesů a přidružená připojení produktu IBM MQ .

Další informace o názvu aplikace a instancích aplikace viz Koncepty vývoje aplikací.

Opakovaně připojitelní klienti

Znovu připojitelné klienty lze přesunout, aby se dosáhlo rovnoměrné distribuce pracovní zátěže, zatímco nepřipojitelného klienta nelze podle definice znovu připojit k jinému správci front. Stále však může existovat dobrý důvod pro připojení nepřipojitelného klienta k jednotnému klastru: Například proto, že klient vytváří určitou formu trvalého stavu a jiný mechanizmus se používá k zajištění toho, že existují instance aplikace spuštěné v jednotlivých správcích front.

Lokálně vázané aplikace

Očekává se, že jednotné klastry budou mít aplikace IBM MQ , které se připojují jako klientské aplikace, spíše než lokálně vázané aplikace. Lokálně vázaným aplikacím není bráněno v připojení ke členům uniformního klastru, ale uniformní klastry nemohou dosáhnout rovnoměrné distribuce pracovní zátěže s lokálně vázanými aplikacemi, protože se nemohou připojit k žádnému jinému členovi klastru.

Související úlohy

Určení názvu aplikace v podporovaných programovacích jazycích

Multi *Automatické vyvažování aplikací*

Automatické vyvažování aplikací výrazně rozšiřuje distribuci a dostupnost aplikací tím, že umožňuje jednotnému klastru IBM MQ pečlivě spravovat distribuci aplikací v rámci klastru a nespoléhat se na randomizaci ani na ruční připnutí aplikací ke specifickým správcům front.

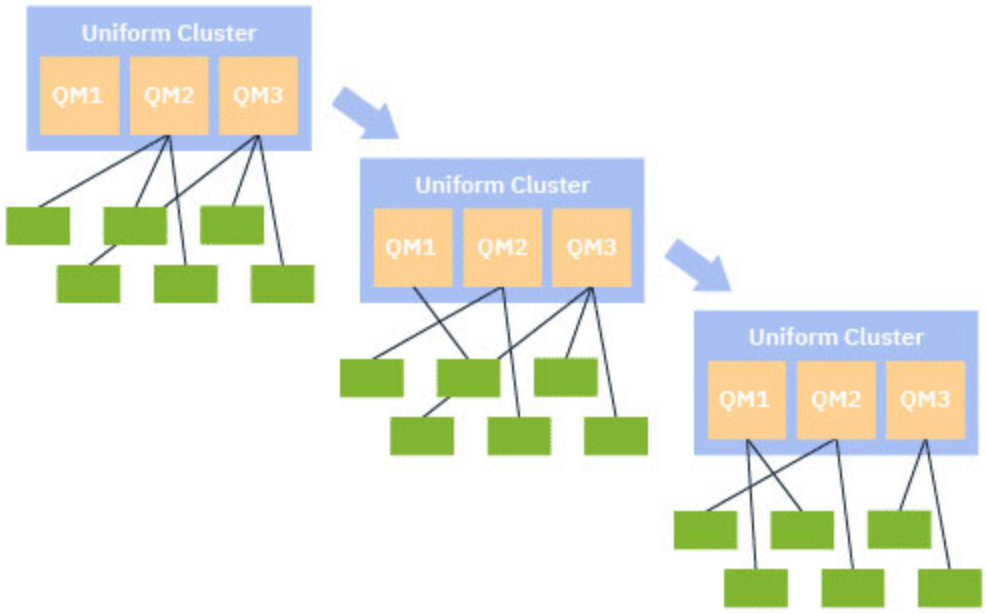
V produktu IBM MQ 9.2.0je automatické vyrovnávání v rámci sady klastrovaných správců front podporováno pro aplikace napsané v jazyce C, JMS, IBM MQ .NET, XMS .NET.

Pokud existuje alespoň tolik instancí stejné aplikace, kolik existuje správců front, jednotný klastr trvale zajistí, že každý správce front bude mít připojenou alespoň jednu instanci aplikace.

Aplikace mohou odebrat specifickou afinitu ke správci front a místo toho použít tabulku CCDT (Client Channel Definition Table) k bezpečnému náhodnému připojení ke skupině správců front v jednotném klastru. Aplikace to mohou provést z následujících důvodů:

- Je-li k dispozici dostatek spotřebujících instancí aplikace, vždy existuje instance aplikace, která zpracovává zprávy.
- Při zastavení správce front jsou všechny připojené instance aplikací rovnoměrně rozděleny mezi zbývající správce front v klastru.
- Při spuštění správce front jsou všechny instance aplikací připojené k jiným správcům front v klastru automaticky vyváženy tak, aby zahrnovaly nově spuštěného správce front.

To znamená, že jednotný klastr neustále zajišťuje optimální distribuci aplikací a maximalizaci zpracování zpráv, a to i v případě plánovaných a neplánovaných výpadků.



Aby bylo dosaženo automatického vyvážení, správci front v jednotném klastru mezi sebou pravidelně sdílejí informace. To lze provést publikováním metadat v tématech systému ve vyhrazené větvi $SYS/MQ stromu témat. Každý správce front v jednotném klastru odebírá zprávy publikované jinými správci front a vytváří obraz stavu aplikací v jednotném klastru.

Správci front monitorují distribuci aplikací klienta v rámci celého klastru. Je-li počet aplikací připojených ke specifickému správci front dostatečně nízký, aby bylo možné určit, že klastr není vyvážený, publikuje tento správce front požadavek na téma systému pro jednoho z ostatních správců front v klastru.

Když je zpráva přijata, cílový správce front požádá jednu ze svých klientských aplikací o přesměrování na požadujícího správce front. Klientská aplikace obdrží požadavek na přesměrování, zavře připojení a znovu se připojí k požadujícímu správci front. Tento mechanismus automatického vyvažování je pro aplikaci transparentní. Další informace viz téma “Jak funguje automatické vyvažování” na stránce 404.

Pravidelnou distribucí metadat o připojených aplikacích může jednotný klastr v průběhu času dosáhnout široce vyváženého poměru klientských aplikací ke správcům front. Aby se zabránilo rychlému následnému přesměrování událostí, algoritmus automatického vyvážení omezuje rychlost, jakou jsou prováděny požadavky na přesměrování.

Můžete monitorovat aktuální stav aplikací v rámci správců front v klastru a instance aplikací. Další informace naleznete v tématu Monitorování vyvažování aplikací. Můžete také vyřešit různé problémy s vyvažováním aplikací, jak je popsáno v tématu Odstraňování problémů s vyvažováním aplikací.

Opětovné vyvážení je užitečné pouze pro aplikace s dlouhou dobou připojení. Máte-li klientské aplikace s krátkými dobami připojení, například klientské aplikace, které jsou zapsány pro pravidelné připojování

a odpojování od různých správců front, měli byste je konfigurovat tak, aby je nebylo možné znovu připojit. Tím dojde k jejich odebrání ze sady aplikací, které se správci front pokoušejí vyvážit.

Související pojmy

“Jak automatické vyvažování používá automatické opětovné připojení” na stránce 406
Od produktu IBM MQ 9.2.0jednotné automatické vyvážení klastru využívá vylepšení stávající funkce automatického opětovného připojení produktu IBM MQ.

Multi *Jak funguje automatické vyvažování*

V jednotném klastru jsou klientská připojení seskupena podle názvu aplikace. Aplikace, které se připojují k libovolnému členovi jednotného klastru s použitím stejného názvu aplikace, jsou považovány za ekvivalentní s jinými aplikacemi používajícími stejný název aplikace.

Automatické vyvážení zajišťuje rovnoměrné rozložení instancí aplikací mezi členy klastru; další informace viz “Názvy aplikací a instance aplikací” na stránce 402 . Pomocí příkazu DISPLAY APSTATUS můžete zobrazit stav jedné nebo více aplikací a instancí aplikací připojených ke správci front nebo jednotnému klastru.

Můžete například nastavit všechny instance aplikace požadavku na pojištění tak, aby měly název aplikace "INSURANCE.REQUESTS". Související připojení z této aplikace budou automaticky seskupena do instancí, kde to bude vhodné, s veškerým vyvážením provedeným na základě jednotlivých instancí.

Když se nové instance aplikace připojí ke členovi jednotného klastru, algoritmus automatického vyvážení vyhodnotí, kteří správci front mají nejméně instancí INSURANCE.REQUESTS a přesměruje některá připojení k těmto správcům front.

Automatické vyvážení je povoleno pouze za následujících okolností:

- Hodnota SHARECNV kanálu je větší než nula.
- Platí jedna z následujících možností:
  - Klientská aplikace uvádí MQCNO_RECONNECT
  - Soubor `mqclient.ini` uvádí **`Defrecon`**=YES

Poznámka: Aplikace s afinitou správce front-například kvůli trvalému odběru nebo dynamické odpovědi na frontu-nelze bezpečně vyvážit a měly by buď použít volbu MQCNO_RECONNECT_QMGR, nebo vůbec žádnou volbu opětovného připojení.

Je-li klient přesměrován na alternativního správce front, použije jako obvykle k vyhledání informací o připojení pro nový cíl lokální tabulky definic kanálů klienta (CCDT). Pro hladký a efektivní provoz automatického vyvážení je proto důležité, aby klienti používali tabulky CCDT obsahující položku pro každého člena jednotného klastru a také všechny skupiny správců front používané k vyvážení počátečních připojení.

Zjednodušuje to použití formátu JSON CCDT, protože umožňuje více připojení pomocí stejného názvu připojení serveru. Další informace viz téma “Konfigurace formátu JSON CCDT” na stránce 44.

Související pojmy

“Jak automatické vyvažování používá automatické opětovné připojení” na stránce 406
Od produktu IBM MQ 9.2.0jednotné automatické vyvážení klastru využívá vylepšení stávající funkce automatického opětovného připojení produktu IBM MQ.

ALW *Automatické vyvažování aplikací JMS*

Když jsou aplikace Jakarta Messaging 3.0 nebo Java Message Service 2.0 automaticky vyváženy, základní skupiny připojení IBM MQ , které aplikace JMS vytvářejí, jsou přesunuty dohromady.

V 9.3.0 V produktu IBM MQ 9.3.0je vlastnost **`dynamicallyBalanced`** k dispozici při konfiguraci ActivationSpecs. Tato vlastnost určuje, zda lze požadovat, aby objekt MDB přijímal zprávy od jiného správce front v rámci vyrovnávání aplikací v jednotném klastru. Další informace naleznete v tématu Konfigurace adaptéru prostředků pro příchozí komunikaci.

Pro obsluhu připojení JMS mají jednotné klastry koncepci *instance aplikace*. Pro systém JMSje *instance aplikace* definována jako JMS Připojení a všechny přidružené relace JMS .

Jedinečná značka připojení je přidělena na připojení klienta, které odpovídá připojení JMS , a stejná značka se pak použije na připojení klienta, která odpovídají relacím JMS vytvořeným tímto připojením JMS .

Pokud například dvojice klientských aplikací spouští aplikace JMS pro jednotný klastr s jedním aktivním správcem front (správce front 1), postupujte takto:

- Klient 1 vytvoří továrnu připojení, na které nastaví název aplikace "App1", a vytvoří JMS Připojení a tři JMS relace. Klient 1 vytvoří ve správci front 1 čtyři připojení klienta, z nichž každé sdílí stejnou značku připojení, a to je považováno za jedinou instanci "App1".
- Klient 2 také vytvoří továrnu připojení, na které nastaví název aplikace "App1", a vytvoří JMS Připojení a dvě JMS relace. Klient 2 vytvoří tři klientská připojení, z nichž každé sdílí stejnou značku připojení (odlišnou od té, která byla přiřazena Zákazníkovi 1), a to je považováno za jedinou samostatnou instanci "App1".
- Správce front tedy vidí dvě instance "App1".

Při provádění automatického vyvážení jsou instance aplikace přesunuty. Správce front zvolí instanci aplikace (skupinu připojení klienta sdílející stejnou značku připojení) a vyžádá si přesun instance do jiného správce front. Kód klienta přijme požadavek a zajistí, aby se všechna související připojení (odpovídající JMS Připojení a jeho přidruženým JMS relacích) přesunovala do nového správce front.

Vezměte například sadu dříve navržených instancí aplikace a předpokládejme, že se v jednotném klastru spustí nový správce front (správce front 2).

Správce front 2 nemá žádnou práci, ale správce front 1 má 2 instance "App1", takže správce front 2 požaduje, aby správce front 1 přenesl instanci "App1" do správce front 2.

Správce front 1 zvolí instanci "App1", která má být přesunuta. Pro účely tohoto příkladu předpokládejme, že si zvolí instanci vytvořenou Zákazníkem 1.

- Správce front 1 odešle klientovi 1 požadavek na přesun jeho instance "App1" do QM2.
- Klient uzavře svá čtyři existující klientská připojení ke správci front 1 a vytvoří čtyři nová připojení ke správci front 2.
- JMS Připojení a jeho JMS relace, s výjimkou krátké přestávky ve zpracování, by neměly být normálně rušeny.

Poznámka:

Aplikace může obdržet výjimku JMS , pokud v době přesunu instance aplikace probíhají určité operace.

Výjimka JMS bude mít propojenou výjimku IBM MQ , ze které lze načíst kód příčiny k určení příčiny selhání.

Očekávané kódy příčiny jsou následující:

MQRC_CALL_PŘERUŠENO
K tomu dochází, když je například zpráva, která je trvalá (výchozí v JMS), vložena mimo synchronizační bod, ale operace je přerušena opětovným připojením.

MQRC_BACKED_OUT
K tomu dochází, když je například pokus o vložení zprávy do synchronizačního bodu přerušen opětovným připojením.

Související pojmy

“Jak funguje automatické vyvažování” na stránce 404
V jednotném klastru jsou klientská připojení seskupena podle názvu aplikace. Aplikace, které se připojují k libovolnému členovi jednotného klastru s použitím stejného názvu aplikace, jsou považovány za ekvivalentní s jinými aplikacemi používajícími stejný název aplikace.

“Jak automatické vyvažování používá automatické opětovné připojení” na stránce 406

Od produktu IBM MQ 9.2.0jednotné automatické vyvážení klastru využívá vylepšení stávající funkce automatického opětovného připojení produktu IBM MQ.

Multi *Jak automatické vyvažování používá automatické opětovné připojení*

Od produktu IBM MQ 9.2.0jednotné automatické vyvážení klastru využívá vylepšení stávající funkce automatického opětovného připojení produktu IBM MQ.

Ve verzích produktu IBM MQ před IBM MQ 9.2.0se funkce automatického opětovného připojení automaticky znovu připojí k rezervní instanci správce front nebo k jinému správci front na základě zadaných podrobností připojení, obvykle seznamu názvů připojení nebo tabulky CCDT (Client Channel Definition Table).

Klient IBM MQ provádí za určitých okolností bezobslužně opětovné připojení, aniž by si aplikace uvědomila, že k němu došlo. Rozhodnutí, ke kterému správci front se má znovu připojit, je zcela v pořadí názvů připojení v seznamu názvů připojení nebo v konfiguraci vyrovnávání pracovní zátěže v tabulce CCDT.

Od produktu IBM MQ 9.2.0 je možné, aby byl požadavek na opětovné připojení odeslán klientovi obsahujícímu pokyn, ke kterému správci front se má klient znovu připojit. V mnoha scénářích opětovného připojení, jako je například selhání správce front nebo administrátor zadávající příkaz **endmqm -r**, není název správce front uveden v informacích pokynů a chování automatického opětovného připojení funguje tak, jak aktuálně funguje.

Pokud jste však nakonfigurovali jednotný klastr, automatické vyrovnávání aplikací pravidelně odesílá klientům požadavky na opětovné připojení, aby se dosáhlo vyváženého klastru. V těchto případech určuje uniformní klastr v pokynu pro opětovné připojení název správce front, aby se zajistilo, že připojení klienta budou přesunuta do správců front, kteří mají nejméně připojení.

Pro automatické vyvažování je důležité, aby:

- Aplikace IBM MQ používají k načtení informací o připojení tabulky CCDT.
- Tabulky CDT obsahují položku pro každého správce front v jednotném klastru.

Pokud tomu tak není, není možné, aby klastr automaticky vyvážil aplikace ve všech členech klastru.

Pokud aplikace používá verzi klienta IBM MQ , která je starší než produkt IBM MQ 9.2.0, a je konfigurována tak, aby podporovala automatické opětovné připojení klienta, může jí být odeslán požadavek uniformního klastru na provedení kroků opětovného připojení.

Klient nebude vyzván k opětovnému připojení ke specifickému správci front, ale místo toho projde stejnou posloupností logiky opětovného připojení, kterou by provedl pro jiné události opětovného připojení. Je možné dosáhnout rovnoměrné distribuce klientských aplikací před produktem IBM MQ 9.2.0 v rámci jednotného klastru tím, že zajistíte, aby klienti byli konfigurováni tak, aby používali tabulky CCDT obsahující rovnoměrně vážené položky pro každého člena klastru.

Aplikace mohou před připojením ke správci front, který potřebuje další instanci, provést několik pokusů o opětovné připojení, a proto se jedná o méně efektivní způsob, jak dosáhnout rovnoměrné distribuce aplikací v rámci klastru. Automatické vyvažování může v těchto prostředích trvat déle.

Klienti IBM MQ nepodporující automatické opětovné připojení klienta

Pokud aplikace používá verzi klienta IBM MQ , která nepodporuje automatické opětovné připojení klienta, může aplikace obdržet návratový kód selhání z volání MQI.

Pokud vaše aplikace nebyla navržena tak, aby zpracovávala selhání a prováděla opětovné připojení ručně, může být nutné pro tyto aplikace zakázat automatické vyvažování.

Poznámka: Automatické vyvážení je povoleno pro jakoukoli aplikaci, která je identifikována jako znovu připojitelná, to znamená, že aplikace má ve svých efektivních volbách připojení MQCNO_RECONNECT.

Související úlohy

“Vytvoření nového uniformní klastru” na stránce 414
Jak vytvoříte nový jednotný klastr.

Multi V 9.3.0 ***Ovlivňování opětovného vyvážení aplikací v uniformních klastrech***

V případě automatického vyrovnávání aplikací (funkce uniformních klastrů) může být připojení aplikace požádáno o přesun do alternativního správce front v libovolném okamžiku životního cyklu.

Úvod

V produktu IBM MQ 9.3.0se algoritmus vyvažování automaticky pokouší vzít v úvahu stav aplikací, aby se minimalizovalo narušení toku aplikací. Tuto volbu lze vyladit tak, aby vyhovovala konkrétním aplikacím nebo instancím aplikací, a to tak, že získáte IBM MQ další informace o typu aplikace nebo vzoru aktivity produktu IBM MQ , kterou tato aplikace provádí.

Osoba, která vyvíjí nebo implementuje klientskou aplikaci, bude obvykle nejlépe schopna porozumět tomuto vzoru a poskytnout tyto informace správci front (viz téma Implementace flexibilních a rozšiřitelných klientských aplikací), ale může být také vyladěna administrátorem.

Uvědomte si, že pokud se správci front nepodaří dosáhnout rovnoměrné distribuce aplikací za rozumnou dobu, je možné, že připojení aplikací budou nadále vyvážena k jiným správcům front bez čekání na vhodnou dobu v jejich toku IBM MQ .

To může být také vyladěno tak, aby splňovalo požadavky. Pokud je důležitější rychle dosáhnout rovnoměrné distribuce aplikací, můžete nakonfigurovat produkt tak, aby čekal méně času na nalezení vhodného času na vyvážení aplikace. Alternativně, pokud je důležitější zabránit narušení aplikací, je možné nakonfigurovat produkt tak, aby vždy čekal na vhodný čas na přesun aplikace.

Další informace naleznete v tématu Implementace flexibilních a rozšiřitelných klientských aplikací .

Další informace o aplikacích .NET naleznete v části “Ovlivnění opětovného vyvážení aplikací v produktu .NET” na stránce 410 .

Pro.XMS.NET , další informace viz Vlastnosti ConnectionFactory .

V 9.3.4 V případě aplikací JMS viz “Ovlivnění opětovného vyvážení aplikací v produktu IBM MQ classes for JMS” na stránce 411 , kde získáte další informace.

Výchozí chování vyvažování aplikací

Standardně je transakce/jednotka pracovního stavu interakce aplikací se správcem front brána v úvahu pro všechny aplikace.

V případě lokálních transakcí se automatické vyvažování aplikací vyhýbá vydávání požadavků na nové vyvažování pro aplikace, které jsou aktuálně zapojeny do transakce. I když to nevylučuje možnost, že aplikace obdrží zálohovaný návratový kód, protože dosažení nakonfigurovaného časového limitu opětovného vyvážení nebo skutečný výpadek by stále mohl způsobit takový návratový kód, znamená to, že aplikace nebudou obvykle požádány o opětovné připojení, zatímco jsou ve středu transakce.

V případě aplikací, které zahájí novou transakci téměř okamžitě po dokončení předchozí transakce, může dojít k prodlevě pro počáteční volání v nové transakci při dokončení opětovného vyvážení. Tím je zajištěno, že automatické vyvažování aplikací je stále schopno dosáhnout rovnoměrné distribuce aplikací mezi správci front v jednotném klastru.

Máte-li aplikace, které používají déle běžící transakce, možná budete chtít zvážit zvýšení hodnoty časového limitu opětovného vyvážení, nebo toto omezení zcela zakázat. Viz “Konfigurace chování vyvažování” na stránce 408 , kde naleznete odkazy, jak to řídit v MQI a .NET, nebo 'Návrh aplikací klienta pro odolnost proti poruchám a rozšiřitelnost' pro ekvivalent úrovně kódu.

Vyvažování požadavek-odpověď

Je-li typ aplikace uveden jako **`Request-Reply`**, očekává se jedna odezva GET pro každou operaci PUT, kterou provádí instance aplikace. Pokud instance aplikace zahrnuje více podprocesů nebo se zabývá požadavky a odezvami v dávkách, více požadavků a odezev může být v daném čase v letu.

Aplikace není považována za způsobilou k přesunu, dokud se počet odeslaných požadavků nerovná počtu přijatých odpovědí nebo dokud není překročena hodnota časového limitu backstop.

Výjimkou je situace, kdy je pro zprávu požadavku nakonfigurováno vypršení platnosti zprávy. Předpokládá se, že odpovědi by měly být přijaty v rámci intervalu vypršení platnosti zprávy požadavku, a když vypršela platnost všech zpráv požadavku, algoritmus vyvážení již nečeká na další odpovědi před tím, než bude instance považována za způsobilou k přesunu.

Je-li nevyřízeno více požadavků, bude se brát v úvahu pouze poslední vypršení platnosti mezi odeslanými zprávami požadavků. Když se používají smysluplné hodnoty vypršení platnosti, měli byste nakonfigurovat parametr vyvážení **Timeout** pro aplikaci tak, aby byl alespoň stejně vysoký jako jakékoli vypršení platnosti odeslané zprávy, abyste se vyvarovali zkratu jakéhokoli očekávaného okna vypršení platnosti požadavku/odezvy.

Předchozí vzor je vhodný pouze pro aplikace, které očekávají, že budou mít období, ve kterých neexistují žádné nevyřízené požadavky. Složité vícevláknové aplikace, které například neustále odesílají a přijímají zprávy, nemusí být nikdy vhodné pro opětovné vyvážení podle tohoto vzoru.

Notes:

- Nebyl učiněn žádný pokus o korelaci specifických požadavků a odpovědí, takže pokud vyprší platnost dřívější odpovědi v rámci dávky v letových zprávách, aplikace může stále čekat, dokud nevyprší platnost posledního požadavku, než bude způsobilá k vyvážení.
- Zejména je třeba věnovat pozornost kombinování neomezeného času vypršení platnosti a ukončení platnosti zpráv, a to z podobných důvodů.

  Pokud jsou nevyřízené zprávy s omezeným vypršením platnosti a nové zprávy jsou odesílány s neomezeným časem vypršení platnosti, *není* neomezený časový limit zohledněn algoritmem vyvažování, který i nadále ctí aktuální nejnovější čas vypršení platnosti.

  Jinak by dřívější odpovědi, které vypršely, mohly zabránit tomu, aby se aplikace vůbec mohla přesunout. Pokud jsou tedy nevyřízené odpovědi s neomezeným časovým limitem vypršení platnosti, ale požadavky s ukončením platnosti jsou následně odeslány, doba čekání se zkrátí na nejdelší (omezené) vypršení platnosti.

  Obecně byste se měli vyhnout tomu, aby jedna instance aplikace odesílala ve vyvážené aplikaci jak zprávy s vypršením platnosti, tak zprávy s vypršením platnosti, protože pro vývojáře nebo administrátora je stále obtížnější přesně sledovat nebo definovat způsobilost k vyvážení.
- Pouze čas vypršení platnosti určený odesílající aplikací (například v rozhraní MQI hodnota MQMD.**Expiry**) se zvažuje při určování, jak dlouho se má čekat na odpovědi. Následné úpravy této hodnoty, například použití CAPEXPRY neovlivní dobu čekání.

Konfigurace chování vyvažování

Chcete-li přesně ovlivnit situaci, kdy produkt IBM MQ znovu vyvažuje aplikace, mohou určitá prostředí klientských aplikací v době připojení poskytovat informace o použitém vzoru systému zpráv.

Tyto informace jsou poskytovány v nové struktuře, která se nazývá *Volby vyvažování*.

Informace o rozhraní MQI viz “Konfigurace chování vyvažování pomocí rozhraní MQI” na stránce 408.

Ekvivalent této struktury pro klienta .NET viz “Ovlivnění opětovného vyvážení aplikací v produktu .NET” na stránce 410.

V 9.3.4 Chcete-li získat přístup JMS k nastavení těchto voleb, prohlédněte si téma “Ovlivnění opětovného vyvážení aplikací v produktu IBM MQ classes for JMS” na stránce 411 , kde získáte další informace.

Jiná klientská prostředí v současné době nepodporují poskytování této struktury v době připojení.

Multi V 9.3.0 *Konfigurace chování vyvažování pomocí rozhraní MQI*

Chcete-li přesně ovlivnit situaci, kdy produkt IBM MQ znovu vyvažuje aplikace, mohou určitá prostředí klientských aplikací v době připojení poskytovat informace o použitém vzoru systému zpráv.

V rozhraní MQI se struktura voleb vyvážení nazývá MQBNO.

Pokud ve vašem programu nejsou poskytnuty žádné *Volby vyvažování* , odvodí podporující klienti tyto informace v sekci Sekce aplikace nebo v sekci ApplicationDefaults v souboru `client.ini` implementovaném společně s klientskou aplikací.

Poznámka: Tyto sekce jsou identické, kromě toho, že verze `Application` obsahuje pole **`Name`** , které identifikuje, na kterou aplikaci se tyto volby vztahují.

Pokud je zadána kterákoli forma sekce, musí být přítomna všechna pole kromě **`BalanceOptions`** , u kterých se předpokládá, že jsou `none` , pokud nejsou explicitně nastavena.

Pořadí, v jakém se volby dodávají, je:

1. Struktura MQBNO je dodána aplikací na CONNX a použita jako celek.
2. Nebo odpovídající sekce s názvem `Application` , je-li přítomna, se používá pouze ke generování jedné
3. Nebo se sekce `ApplicationDefaults` , je-li přítomna, používá pouze ke generování
4. Nebo žádné toky MQBNO pro toto připojení.

Můžete dodat tři klíčové části informací ze struktury MQBNO nebo ze souboru `client.ini` :

1. **`ApplicationType`** nebo vzor aplikace.

   Toto pole označuje IBM MQ obecný vzor aktivity IBM MQ , které se tato aplikace účastní.

   Podporovány jsou tři typy aplikací:

   Jednoduché
   Za výchozími hodnotami popsanými v části “Výchozí chování vyvažování aplikací” na stránce 407 by neměla být použita žádná specifická pravidla.

   Požadavek-odpověď
   Po každém volání MQPUT je pro zprávu odpovědi očekáváno odpovídající volání MQGET. Další podrobnosti viz “Vyvažování požadavek-odpověď” na stránce 407.

   Spravovaný klient
   Požadavky na opětovné vyvážení jsou vždy okamžitě odesílány klientovi, který je znovu vyvažuje v bodě, který považuje za vhodný, například adaptér prostředků JEE by se tímto způsobem registroval.
2. **`Timeout`** , po kterém může opětovné vyvážení přerušit aktivitu aplikace
3. Specifický **`BalanceOptions`**

Příklady, kdy může být vaše aplikace znovu vyvážena

Příklad 1

Napsali jste aplikaci, která vkládá zprávy do synchronizačního bodu a potvrzuje dávku zpráv vyvoláním volání MQCMIT. Po dokončení volání MQCMIT aplikace začne vkládat zprávy do nového synchronizačního bodu.

Navrhovaná konfigurace IBM MQ
Dostatečné výchozí volby

Výsledek
Instance aplikace je přesunuta po úspěšném (nebo neúspěšném) volání MQCMIT po splnění konfigurovaného počtu transakcí.

Standardně, pokud dávka zpráv překročí 10 sekund, může být odvolána, pokud bylo požadováno vyvážení. Pokud očekáváte, že transakce budou pravidelně překračovat tento limit a budou vyžadovat povolení tohoto limitu, můžete odpovídajícím způsobem rozšířit **`Timeout`** .

Příklad 2

Po zpracování požadavku jste napsali aplikaci, která vkládá jednu zprávu do instance fronty klastru, a jiná aplikace odpoví na lokální dočasnou dynamickou frontu se zprávou. Když byl požadavek destruktivně načten z lokální fronty, aplikace vloží svou další zprávu požadavku.

Navrhovaná konfigurace IBM MQ
Nastavte Typ na MQBNO_BALTYPE_REQREP

Výsledek
Instance aplikace je přesunuta, když aplikace dokončí volání MQGET. V tomto okamžiku se instance aplikace přesune do jiného správce front. Všechna následná volání MQPUT se provádějí v novém správci front.

MQBNO
ApplicationType

Multi V 9.3.0 *Ovlivnění opětovného vyvážení aplikací v produktu .NET*
V produktu IBM MQ 9.3.0jsou k dispozici další konstanty pro nastavení vlastností volby vyvážení pomocí hašovací tabulky z aplikace, když používáte třídu `MQQueueManager` pro připojení ke správci front.

Následující konstanty se používají k ovlivnění vyvážení aplikací v produktu .NET:

Opětovné vyvážení typu aplikace
Typ akce vyvážení; reprezentovaný konstantou **`MQC.BALANCING_APPLICATION_TYPE_PROPERTY`**

- Tuto vlastnost musíte použít k nastavení pole **`ApplicationType`** struktury MQBNO.

  Musíte nastavit hodnoty typu integer a možné hodnoty jsou:

  MQC.BALANCING_APPLICATION_TYPE_SIMPLE
  Jednoduché vyvážení; kromě pravidel popsaných v části “Ovlivňování opětovného vyvážení aplikací v uniformních klastrech” na stránce 407se nepoužívají žádná specifická pravidla. Toto je výchozí hodnota.

  MQC.BALANCING_APPLICATION_TYPE_REQUEST_REPLY
  Vyvažování požadavek-odpověď; po každém volání **MQPUT** je pro zprávu odpovědi očekáváno odpovídající volání **MQGET** . Vyvažování je zpožděno, dokud není taková zpráva přijata, nebo dokud není zpráva požadavku **EXPIRY** překročena.

  Pokud je opětovné připojení povoleno aplikací a tato vlastnost není nastavena, použije se hodnota **`MQC.BALANCING_APPLICATION_TYPE_SIMPLE`** .

Volby opětovného vyvážení
Volby vyvážení nastavené vydávající aplikací; reprezentované konstantou **`MQC.BALANCING_OPTIONS_PROPERTY`**

- Tuto vlastnost musíte použít k nastavení pole **`BalanceOptions`** struktury MQBNO.

  Musíte nastavit hodnoty typu integer a možné hodnoty jsou:

  MQC.BALANCING_OPTIONS_NONE
  Nejsou nastaveny žádné volby. Toto je výchozí hodnota

  MQC.BALANCING_OPTIONS_IGNORE_TRANSACTIONS
  Nastavení této volby umožňuje vyvážit aplikace i v případě, že se nacházejí uprostřed transakce.

  Pokud je opětovné připojení povoleno aplikací a tato vlastnost není nastavena, použije se hodnota **`MQC.BALANCING_OPTIONS_NONE`** .

Časový limit opětovného vyvážení
Časový limit, po kterém může nové vyvážení přerušit aktivitu aplikace; reprezentováno konstantou **`MQC.BALANCING_TIMEOUT_PROPERTY`**

- Tuto vlastnost musíte použít k nastavení pole Časový limit struktury MQBNO.

  Musíte nastavit hodnoty typu integer a možné hodnoty jsou:

  MQC.BALANCING_TIMEOUT_AS_DEFAULT
  Nastavená výchozí hodnota časového limitu. Toto je výchozí hodnota

MQC.BALANCING_TIMEOUT_IMMEDIATE
Dojde k okamžitému vypršení časového limitu

MQC.BALANCING_TIMEOUT_NEVER
Žádný časový limit se nevyskytne

Poznámka: Musíte zadat pouze jednu hodnotu z definovaných hodnot, nebo hodnotu 0-999999999 sekund.

Implementace flexibilních a rozšiřitelných klientských aplikací
MQBNO

Multi V 9.3.4 *Ovlivnění opětovného vyvážení aplikací v produktu IBM MQ classes for JMS*

V systému IBM MQ 9.3.4jsou k dispozici další konstanty pro nastavení vlastností volby vyvážení v systému **ConnectionFactory**. Tyto konstanty lze použít pouze v případě, že je parametr **WMQ_PROVIDER_VERSION** nastaven na hodnotu 7. Aplikace `Request_reply` v jednotném klastru musí umožňovat zmeškání odpovědí.

- “Dostupné konstanty” na stránce 411.
- “Potenciál ztracených zpráv při vyvažování aplikací REQUEST_REPLY” na stránce 412.

Dostupné konstanty

Následující konstanty se používají k ovlivnění vyvážení aplikací v produktu IBM MQ classes for JMS:

Opětovné vyvážení typu aplikace
Typ akce vyvážení; reprezentovaný konstantou **WMQConstants.WMQ_BALANCING_APPLICATION_TYPE**

- Tuto vlastnost musíte použít k nastavení pole **ApplicationType** struktury MQBNO .

  Musíte nastavit hodnoty typu integer. Toto jsou možné hodnoty:

  WMQConstants.WMQ_BALANCING_APPLICATION_TYPE_SIMPLE (Výchozí)
  Jednoduché vyvážení; kromě pravidel popsaných v části “Ovlivňování opětovného vyvážení aplikací v uniformních klastrech” na stránce 407se nepoužívají žádná specifická pravidla.

  WMQConstants.WMQ_BALANCING_APPLICATION_TYPE_REQUEST_REPLY
  Vyvažování požadavek-odpověď; po každém volání **MQPUT** je pro zprávu odpovědi očekáváno odpovídající volání **MQGET** . Vyvažování je zpožděno, dokud není taková zpráva přijata, nebo dokud není zpráva požadavku **EXPIRY** překročena.

  Pokud aplikace povolí opětovné připojení a tato vlastnost není nastavena, použije se hodnota **WMQConstants.WMQ_BALANCING_APPLICATION_TYPE_SIMPLE** .

Volby opětovného vyvážení
Volby vyvážení nastavené vydávající aplikací; reprezentované konstantou **WMQConstants.WMQ_BALANCING_OPTIONS**

- Tuto vlastnost musíte použít k nastavení pole **BalanceOptions** struktury MQBNO .

  Musíte nastavit hodnoty typu integer. Toto jsou možné hodnoty:

  WMQConstants.WMQ_BALANCING_OPTIONS_NONE (Výchozí)
  Nejsou nastaveny žádné volby.

  WMQConstants.WMQ_BALANCING_OPTIONS_IGNORE_TRANSACTIONS
  Nastavení této volby umožňuje vyvážit aplikace i v případě, že se nacházejí uprostřed transakce.

  Pokud aplikace povolí opětovné připojení a tato vlastnost není nastavena, použije se hodnota **WMQConstants.WMQ_BALANCING_OPTIONS_NONE** .

Časový limit opětovného vyvážení
Časový limit, po kterém může nové vyvážení přerušit aktivitu aplikace; reprezentováno konstantou **WMQConstants.WMQ_BALANCING_TIMEOUT**

- Tuto vlastnost musíte použít k nastavení pole **Timeout** struktury MQBNO .

Musíte nastavit hodnoty typu integer. Toto jsou možné hodnoty:

WMQConstants.WMQ_BALANCING_TIMEOUT_AS_DEFAULT (Výchozí)
Nastavená výchozí hodnota časového limitu. Standardně je tato hodnota 10 sekund.

WMQConstants.WMQ_BALANCING_TIMEOUT_IMMEDIATE
Dojde k okamžitému vypršení časového limitu.

WMQConstants.WMQ_BALANCING_TIMEOUT_NEVER
Nevyskytne se žádný časový limit.

hodnota mezi 1 a 999999999
Představuje hodnotu v sekundách.

Poznámka: Musíte zadat pouze jednu hodnotu z definovaných hodnot, nebo hodnotu 0-999999999 sekund.

Tyto vlastnosti lze nastavit také v reprezentacích rozhraní JNDI továren připojení pomocí rozhraní `JMSAdmin` nebo IBM MQ Explorer .

Potenciál ztracených zpráv při vyvažování aplikací REQUEST_REPLY

V produktu IBM MQ classes for JMS (a IBM MQ classes for Jakarta Messaging) je funkčnost požadavek/odpověď implementována nastavením vlastnosti **JMSReplyTo** ve zprávě požadavku, kterou používá odpovídající aplikace k určení, zda je odpověď odeslána. V JMS termínech je vlastnost **JMSReplyTo** `Destination`.

Při překladu do operací IBM MQ je vlastnost **JMSReplyTo** odeslána jako úplný identifikátor URI fronty identifikující frontu ve specifickém správci front.

Vzhledem k asynchronní povaze zpracování opětovného vyvažování připojení může být opětovné připojení zahájeno poté, co byla vlastnost **JMSReplyTo** přeložena na úplný identifikátor URI, ale před vložením zprávy požadavku do fronty požadavků. Za těchto okolností může odpovídající aplikace odeslat svou odpověď do původní fronty odpovědí v původním správci front, ale požadující aplikace nyní může čekat na odpověď v novém správci front.

Aplikace systému `Request_reply` v jednotném klastru proto musí umožňovat zmeškání odpovědí.

Implementace flexibilních a rozšiřitelných klientských aplikací
MQBNO-Volby vyvažování

Multi *Omezení a aspekty pro jednotné klastry*

Omezení a další body, které je třeba zvážit při konfiguraci uniformních klastrů.

Poznámka: Obecné požadavky při konfiguraci uniformní klastry viz také “Vytvoření nového uniformní klastru” na stránce 414.

Důležitost uniformity mezi správci front

Standardně může být každá aplikace, která se deklaruje jako `reconnectable` , kdykoli znovu vyvážena do alternativního správce front v jednotném klastru. To znamená, že všechny prostředky, například fronta, téma nebo záznam oprávnění, které jsou vyžadovány těmito aplikacemi, musí být deklarovány ve všech správcích front v jednotném klastru.

Konzistence konfigurace správce front není zajištěna. Je na administrátorovi systému, aby nakonfigurovali členy klastru tak, aby měli podobnou konfiguraci.

Můžete však napomoci konzistenci pomocí funkce Automatická konfigurace ze skriptu MQSC při spuštění ke sdílení skriptů MQSC, které definují objekty pro klastr, a tudíž zajistit, aby všechny měly stejné definice. Další informace viz téma “Vytvoření nového uniformní klastru” na stránce 414.

Tato uniformita se rozšiřuje na správce front úplného úložiště pro klastr. Ačkoli v případě tradičních klastrů IBM MQ je často považováno za nejlepší postup oddělit úplná úložiště na samostatné systémy, v jednotném klastru je model takový, že úplná úložiště se plně podílejí na pracovní zátěži klastru a aplikací procesu spolu s ostatními uzly.

Překrývající se uniformní klastry a tradiční klastry IBM MQ

Správce front uniformního klastru se může účastnit nejvýše jednoho uniformního klastru a může být také členem libovolného počtu standardních klastrů IBM MQ . Může být užitečné uvažovat o jednotném klastru jako o jediném správci front v širším klastru.

Správce front uniformního klastru musí fungovat jako úplné úložiště pouze pro samotný uniformní klastr. Žádného správce front, který patří do uniformního klastru, ale může také patřit do širšího tradičního klastru IBM MQ , nelze použít jako úložiště mimo uniformní klastr. Další informace naleznete v tématu Jak vybrat správce front klastru pro uložení úplných úložišť.

Chcete-li nahradit jednoho správce front úplného úložiště jednotným klastrem, oddělte úplné úložiště od práce aplikace, která na něm probíhá, a přesuňte pouze práci aplikace do jednotného klastru.

Používáte-li automatické definice pro jednotné klastry, nelze kanály klastru sdílet pro použití v jiných klastrech, tj. nastavíte atribut **CLUSTER** na automatický klastr a atribut **CLUSNL** musí být prázdný.

Aspekty vyvažování aplikací

Instance aplikace nejsou vždy rovnoměrně vyváženy, zejména za následujících okolností:

- Pokud je v klastru méně instancí aplikace než správců front.
- Během krátké doby poté, co se klientské aplikace připojí ke klastru nebo jej opustí.

Chcete-li zabránit tomu, aby byly klientské aplikace vyváženy příliš často, zejména při příchodu a odchodu připojení aplikací, jsou nastavena omezení týkající se toho, jak často má jednotný klastr aplikace klienta znovu vyvážit. Po období vysoké aktivity připojení nebo odpojení může trvat několik minut, než budou zbývající instance aplikace rovnoměrně vyváženy v rámci jednotného klastru.

Další informace naleznete v tématu Odstraňování problémů s vyrovnáváním aplikací.

Aplikační spřízněnosti

Ne všechny aplikace jsou vhodné pro automatické vyvážení v rámci jednotného klastru. Vyváženy jsou pouze aplikace, které uvádějí parametr **MQCNO_RECONNECT** . Aplikace, které mají afinitu ke konkrétnímu správci front, musí buď zadat volbu **MQCNO_NO_RECONNECT** , nebo **MQCNO_RECONNECT_Q_MGR**. Druhý z nich umožňuje překonání selhání HA, ale ne opětovné vyvážení.

Příklady aplikací, které vytvářejí implicitní afinitu ke správci front:

- Aplikace, které vytvářejí trvalé odběry.
- Aplikace, které vytvářejí trvalé dynamické fronty, například pro příjem zpráv s odpovědí.
- Aplikace, které očekávají striktní řazení zpráv nebo vyžadují všechny zprávy v posloupnosti, budou zpracovány stejnou instancí aplikace nebo obojím.

Tyto aplikace musí uvádět volby **MQCNO_NO_RECONNECT** nebo **MQCNO_RECONNECT_Q_MGR** spíše než **MQCNO_RECONNECT**.

Další informace viz Volby opětovného připojení.

Dostupnost zpráv

Zatímco vyvažování aplikací může znovu vyvážit připojení kolem nezdařených nebo dočasně nedostupných správců front, uniformní klastry nereplikují data zpráv v rámci svých členů. Pro dostupnost dat platí, že pokud dojde k selhání uzlu, musí být každý člen jednotného klastru také nakonfigurován tak, aby byl vysoce dostupný. Je k dispozici mnoho řešení replikace dat a vysoké dostupnosti, která lze kombinovat s jednotnými klastry pro maximální dostupnost služeb a dat, například:

- Replikované úložiště, které podporuje instanci kontejneru, která je automaticky restartována koordinací kontejneru. Další informace naleznete v tématu Jeden správce front schopný obnovy.
- Správci front RDQM. Další informace viz Vysoká dostupnost RDQM.
- Správci front pro více instancí. Další informace naleznete v tématu Správci front s více instancemi.

- Nativní HA. Další informace viz Nativní HA.
- IBM MQ Appliance HA. Další informace naleznete v tématu Vysoká dostupnost.

Rozšiřitelnost a výkon jednotných klastrů

Chcete-li povolit užší integraci a sdílení stavu aplikace mezi správci front v jednotném klastru, je zapotřebí vyšší úroveň interkomunikace než v tradičním klastru IBM MQ . Proto se nedoporučuje škálovat na velký počet správců front v jednom jednotném klastru, protože další komunikace má nepříznivý vliv na výkon.

Z důvodů výkonu i správy je vhodnější uvažovat o jednotném klastru jako o jediném tradičním správci front, který poskytuje systém zpráv pro řadu souvisejících aplikací, ale nejedná se o jedinou službu systému zpráv v rámci podniku. V tomto vzoru jsou malá čísla až 10 správců front obvykle dostatečná pro podporu velkého počtu připojení klientských aplikací. Vyvažování aplikací usnadňuje spouštění s malými čísly, například 3 správci front, a rozšiřování přidáním dalších správců front.

Upozornění: Povolení jednotného chování klastru v klastru, který nemá doporučené charakteristiky, zejména použití klastrů s velkým počtem správců front, bude mít pravděpodobně závažný dopad na výkon.

Související pojmy

"Automatické vyvažování aplikací" na stránce 402
Automatické vyvažování aplikací výrazně rozšiřuje distribuci a dostupnost aplikací tím, že umožňuje jednotnému klastru IBM MQ pečlivě spravovat distribuci aplikací v rámci klastru a nespoléhat se na randomizaci ani na ruční připnutí aplikací ke specifickým správcům front.

ALW Vytvoření jednotného klastru

Můžete zjednodušit počáteční vytvoření jednotného klastru a následně zachovat identickou konfiguraci mezi členy jednotného klastru pomocí automatické konfigurace a podpory automatického klastrování.

Než začnete

Před vytvořením jednotného klastru byste si měli přečíst téma "Omezení a aspekty pro jednotné klastry" na stránce 412.

Informace o této úloze

Určíte, že s konkrétním klastrem IBM MQ se má zacházet jako s jednotným klastrem, dodáním sekce AutoCluster v souboru `qm.ini` s alespoň **Type**=*Uniform* a **ClusterName**=*< jednotný název klastru >*.

Volitelně můžete nakonfigurovat základní klastr IBM MQ pomocí stejné sekce `.ini` pomocí *automatického vytvoření klastru*. Při použití této automatické podpory klastrů k nastavení klastru poskytnete konfigurační soubor, který popisuje klastr a jeho úplná úložiště.

Pokud je spuštěný správce front uveden jako jedno z úplných úložišť, automaticky se z něj stane úplné úložiště. Podobně platí, že když je definován přijímací kanál klastru, jsou odesílací kanály klastru do úplného úložiště nebo úložišť automaticky definovány.

Procedura

Chcete-li využívat další funkce, které vyžadují jednotný klastr, musíte provést jeden z následujících kroků:

- Převést existující klastr na jednotný klastr, který odpovídá vzoru popsanému v části "O jednotných klastrech" na stránce 400.
- Vytvořit nový uniformní klastr pro tento účel.

ALW *Vytvoření nového uniformní klastru*

Jak vytvoříte nový jednotný klastr.

Postup

1. Vytvořte soubor, který popisuje, jak má samotný klastr vypadat z hlediska úplných úložišť.

   Pokud jde o jakýkoli klastr, dvě úplná úložiště fungují jako centrální úložiště informací o klastru.

   Konkrétně musíte popsat názvy a názvy připojení pro dvě úplná úložiště v tomto klastru.

   Poznámka: K tomu dochází před vytvářením čehokoli (včetně správců front) a následující proces níže zahrnuje vytváření těchto správců front.

   Představte si například, že nastavujete jednotný klastr s názvem UNICLUS se členy správce front QMA, QMB, QMC a QMD. V tomto příkladu budou QMA a QMB úplnými úložišti, s QMC a QMD jako částečnými úložišti. Ukázkový konfigurační soubor `uniclus.ini`:

   ```
   AutoCluster:
      Repository2Conname=QMA.dnsname(1414)
      Repository2Name=QMA
      Repository1Conname=QMB.dnsname(1414)
      Repository1Name=QMB
      ClusterName=UNICLUS
      Type=Uniform
   ```

   Pole **RepositoryNConname** se používají jako atribut *conname* pro ostatní členy klastru k definování odesílatelů klastru (CLUSSDR) pro ně a mohou být seznamem připojení pro správce front s více instancemi a volitelně mohou obsahovat port.
2. Vytvořte ukázkový konfigurační soubor `uniclus.mqsc` obsahující definice MQSC, které chcete použít pro všechny členy klastru.

   V tomto souboru je zapotřebí jeden povinný řádek, což je definice přijímacího kanálu klastru (CLUSRCVR) s atributem CLUSTER s automatickým názvem klastru (obvykle prostřednictvím vložení + AUTOCL +) a názvem kanálu, který obsahuje vložení + QMNAME +.

   Tento oddíl popisuje, jak se k jednotlivým správcům front připojují další členové uniformního klastru, a používá se také jako šablona pro připojení k ostatním správcům front. Příkladem definice může být například:

   ```
   define channel('+AUTOCL+_+QMNAME+') chltype(clusrcvr) trptype(tcp)
   conname(+CONNAME+) cluster('+AUTOCL+') replace
   ```

   Při konfiguraci automatických klastrů může definice přijímacího kanálu klastru použít některá další vložení do polí CLUSTER, CONNAME a CHANNEL, aby byla definice identická ve všech správcích front v jednotném klastru. To zahrnuje:

   + AUTOCL +
   Název automatického klastru

   + QMNAME +
   Název vytvářeného správce front

   + JMÉNO +
   Proměnná definovaná během vytváření správce front pomocí parametru **-iv** nebo v sekci `Variables` qm.ini pro použití v řetězci parametru názvu připojení. Název proměnné může být libovolná hodnota.

   Pamatujte si, že názvy kanálů jsou omezeny na 20 znaků, a proto hodnota, která je vložená, stejně jako při nahrazení vložených znaků, musí odpovídat tomuto omezení. Ukázkový soubor může vypadat například takto:

   ```
   *##########################################################################
   * Compulsory section for all uniform cluster queue managers
   *##########################################################################
   define channel('+AUTOCL+_+QMNAME+') chltype(clusrcvr) trptype(tcp) conname(+CONNAME+)
   cluster('+AUTOCL+') replace
   *
   *##########################################################################
   * Configuration for all queue managers
   *##########################################################################
   ```

```
define QL(APPQ) maxdepth(99999999) replace
define QL(APPQ2) maxdepth(99999999) replace
define channel(CLIENTCHL) chltype(svrconn) trptype(tcp) replace
```

3. Zpřístupněte tyto dva soubory na každém počítači, který bude hostitelem člena jednotného klastru.
   Například `/shared/uniclus.ini` a `/shared/uniclus.mqsc`.
4. Na každém z těchto počítačů vytvořte správce front.
   Na příkazovém řádku zadejte:
   a. Požadavek na spuštění modulu listener na očekávaném portu
   b. Požadavek na automatickou konfiguraci INI (**-ii**) ukazující na soubor nastavení automatického klastru (uniclus.ini)
   c. Požadavek na automatickou konfiguraci MQSC (**-ic**) ukazující na konfigurační soubor MQSC, který obsahuje definici CLUSRCVR pro jednotný klastr.
   d. CONNAME pro tohoto správce front.

   Na hostiteli pro QMA:

```
crtmqm -p 1414 -ii /shared/uniclus.ini -ic /shared/uniclus.mqsc -iv
CONNAME=QMA.dnsname(1414) QMA
strmqm QMA
```

   Každý správce front v jednotném klastru je vytvořen s téměř identickým příkazovým řádkem-všechny rozdíly mezi úplným a částečným úložištěm jsou zpracovány automaticky pro jednotný klastr.
   Na hostiteli pro QMB:

```
crtmqm -p 1414 -ii /shared/uniclus.ini -ic /shared/uniclus.mqsc -iv
CONNAME=QMB.dnsname(1414) QMB
strmqm QMB
```

   Na hostiteli pro QMC:

```
crtmqm -p 1414 -ii /shared/uniclus.ini -ic /shared/uniclus.mqsc -iv
CONNAME=QMC.dnsname(1414) QMC
strmqm QMC
```

   Na hostiteli pro QMD:

```
crtmqm -p 1414 -ii /shared/uniclus.ini -ic /shared/uniclus.mqsc -iv
CONNAME=QMD.dnsname(1414) QMD
strmqm QMD
```

   Co se děje automaticky:

   Při spuštění správce front jsou definice ze souboru `uniclus.ini` použity na soubor `qm.ini` . Další informace viz téma “Automatická konfigurace souboru qm.ini při spuštění” na stránce 98. Tím se přidá definice **AutoCluster** do souboru `qm.ini` .

   Pokud je správce front v sekci **AutoCluster** uveden jako jedno z úplných úložišť, bude automaticky převeden na úplné úložiště, podobně jako při zadání příkazu MQSC ALTER QMGR REPOS (**ClusterName**), jinak bude převeden na dílčí úložiště, podobně jako při zadání příkazu MQSC ALTER QMGR REPOS ('').

   Při zpracování definice přijímacího kanálu klastru pro automatický klastr jsou odesílací kanály klastru definovány z tohoto správce front do všech úplných úložišť v sekci **AutoCluster** (s výjimkou lokálního správce front, pokud se jedná o jedno z úplných úložišť). Tyto odesílací kanály dědí všechny atributy obecného kanálu z lokálního příjemce klastru, který byl definován.

   Upozornění: Ačkoli jsou kanály vytvořeny bez dalšího ručního zásahu, jedná se o objekty administrativních kanálů, které lze zobrazit a spravovat jako pro jakoukoli jinou definici kanálu. Tyto objekty byste neměli zaměňovat s odesílacími kanály klastru 'automaticky definovanými', vytvořenými přechodně a na vyžádání klastrem pro směrování provozu zpráv.

Jak pokračovat dále

Ověřte jednotné nastavení klastru

Je-li parametr **ClusterName** správně nastaven a správce front je členem uvedeného klastru, je vydána zpráva AMQ9883 , která potvrzuje, že je klastr nyní identifikován jako uniformní klastr.

Poté můžete použít funkce jednotného klastru, například automatické vyrovnávání aplikací. Pokud byl tento parametr během spouštění správce front nastaven, ale nejedná se o platný název klastru IBM MQ , bude název ignorován a bude vydána chybová zpráva AMQ9882 .

Pokud se jedná o platný název klastru, ale pro identifikovaný klastr neexistují žádné kanály klastru, bude do protokolu chyb správce front vydána varovná zpráva AMQ9881 , která administrátorovi umožní tuto situaci identifikovat a opravit.

Ověření nastavení automatizovaného klastru

Pokud jste k nastavení jednotného klastru použili podporu automatického klastru, můžete ověřit, že správci front uvedení jako úplná úložiště jsou nyní správně nakonfigurováni jako taková, pomocí příkazů runmqsc:

```
QMA:
     1 : dis qmgr repos
AMQ8408I: Display Queue Manager details.
   QMNAME(QMA)                             REPOS(UNICLUS)
```

Vzhledem k tomu, že dílčí úložiště nejsou konfigurována jako úložiště:

```
QMC:
     1 : dis qmgr repos
AMQ8408I: Display Queue Manager details.
   QMNAME(QMC)                             REPOS( )
```

Kromě toho byste měli mít možnost vidět, že odesílací kanály klastru (CLUSSDR) byly konfigurovány z každého správce front do jiných úplných úložišť, s použitím názvu kanálu z konfiguračního souboru MQSC:

```
QMA:
     1 : dis chl(UNICLUS*) conname
AMQ8414I: Display Channel details.
   CHANNEL(UNICLUS_QMA)                    CHLTYPE(CLUSRCVR)
   CONNAME(QMA.dnsname(1414))
AMQ8414I: Display Channel details.
   CHANNEL(UNICLUS_QMB)                    CHLTYPE(CLUSSDR)
   CONNAME(QMB.dnsname(1414))

QMC:
     1 : dis chl(UNICLUS*) conname
AMQ8414I: Display Channel details.
   CHANNEL(UNICLUS_QMA)                    CHLTYPE(CLUSSDR)
   CONNAME(QMA.dnsname(1414))
AMQ8414I: Display Channel details.
   CHANNEL(UNICLUS_QMB)                    CHLTYPE(CLUSSDR)
   CONNAME(QMB.dnsname(1414))
AMQ8414I: Display Channel details.
   CHANNEL(UNICLUS_QMC)                    CHLTYPE(CLUSRCVR)
   CONNAME(QMC.dnsname(1414))
```

Související pojmy

“O jednotných klastrech” na stránce 400
Cílem jednotné implementace klastru je, aby aplikace mohly být navrženy pro škálování a dostupnost a aby se mohly připojovat k libovolným správcům front v rámci uniformního klastru. Tím se odebere jakákoli závislost na specifickém správci front, což povede k lepší dostupnosti a vyrovnávání pracovní zátěže provozu systému zpráv. z/OS Uniformní klastry nejsou k dispozici v systému IBM MQ for z/OS; skupiny sdílení front poskytují mnoho schopností uniformního klastru.

“Omezení a aspekty pro jednotné klastry” na stránce 412

Omezení a další body, které je třeba zvážit při konfiguraci uniformních klastrů.

ALW *Převod existujícího klastru na uniformní klastr*

Pomocí tohoto postupu můžete převést existující klastr na jednotný klastr.

Informace o této úloze

Pokud převedete existující klastr na uniformní klastr, musíte zajistit, aby ve všech členech klastru existovala definice potřebná pro podporu vyrovnávání aplikací mezi správci front.

Postup

1. Povolte odběr publikování IBM MQ včetně vzdáleného (klastrovaného) odběru publikování ve všech správcích front.

   Jedná se o předpoklad pro jednotnou funkčnost klastru, takže musíte zajistit, aby atributy PSMODE a PSCLUS správce front byly nastaveny na výchozí hodnotu ENABLED.
2. Přidejte sekci **AutoCluster** do souboru `qm.ini` k názvu klastru IBM MQ , který se používá v definicích objektů MQSC, například v kanálech klastru.

   Pokud je například název klastru UNICLUS, přidejte nebo upravte sekci AutoCluster v souborech `qm.ini` takto:

   ```
   AutoCluster:
         ClusterName=UNICLUS
       Type=Uniform
   ```
3. Chcete-li použít nové nastavení, restartujte správce front.
4. Zvažte použití automatické konfigurace jako mechanismu pro zajištění toho, aby všichni členové uniformního klastru měli stejnou konfiguraci použitou od spuštění.

   Další podrobnosti viz Automatická konfigurace ze skriptu MQSC při spuštění .

Související pojmy

“O jednotných klastrech” na stránce 400
Cílem jednotné implementace klastru je, aby aplikace mohly být navrženy pro škálování a dostupnost a aby se mohly připojovat k libovolným správcům front v rámci uniformního klastru. Tím se odebere jakákoli závislost na specifickém správci front, což povede k lepší dostupnosti a vyrovnávání pracovní zátěže provozu systému zpráv. z/OS Uniformní klastry nejsou k dispozici v systému IBM MQ for z/OS; skupiny sdílení front poskytují mnoho schopností uniformního klastru.

“Omezení a aspekty pro jednotné klastry” na stránce 412
Omezení a další body, které je třeba zvážit při konfiguraci uniformních klastrů.

Multi Použití automatické konfigurace klastru

Produkt IBM MQ nakonfigurujete tak, aby umožňoval automatickou konfiguraci změnou informací o konfiguraci `qm.ini` .

Poznámka: Sekci AutoCluster můžete použít pouze pro uniformní klastry.

Sekce ke konfiguraci

Můžete změnit následující sekce:

AutoConfig
Definováno v souboru `qm.ini` . Při spuštění správce front identifikuje, které automatické konfigurační soubory se mají použít.

Tento mechanizmus byste měli použít k distribuci identické konfigurace klastru, když se používají jednotné klastry.

AutoCluster
Definováno v souboru `qm.ini` . Používá se, když správce front začne zjišťovat, zda je klastr členem automatického klastru, a může identifikovat úplná úložiště klastru.

Proměnné
Definováno v souboru `qm.ini` . Obsahuje některé proměnné správce front.

Atributy pro sekci AutoConfig

V sekci AutoConfig jsou povoleny následující dva atributy:

MQSCConfig=*< Cesta_ >*
Cesta je buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.mqsc` použity na správce front při každém spuštění správce front.

Další informace naleznete v tématu Automatická konfigurace ze skriptu MQSC při spuštění.

IniConfig=*< cesta_k>*
Cesta je buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.ini` použity na soubor `qm.ini` při každém spuštění správce front.

Další informace viz téma “Automatická konfigurace souboru qm.ini při spuštění” na stránce 98.

Tyto atributy se často používají jako součást nastavení uniformních klastrů. Další informace viz téma “Vytvoření nového uniformní klastru” na stránce 414.

Příklad sekce:

```
AutoConfig:
MQSCConfig=C:\MQ_Configuration\uniclus.mqsc
IniConfig=C:\MQ_Configuration\uniclus.ini
```

Atributy pro sekci AutoCluster

Následující atributy jsou povinné pro sekci AutoCluster :

Typ =*Jednotná*
Určuje typ automatického klastru a jedinou platnou volbou je volba *Jednotný*, která představuje uniformní klastr.

ClusterName=*< Řetězec >*
Název klastru, tj. název automatického klastru.

Přítomnost výše uvedených atributů umožňuje vyvažování aplikací pro jednotné klastry. Další podrobnosti viz “Automatické vyvažování aplikací” na stránce 402 .

Kromě toho lze provést zjednodušené nastavení klastru, pokud je klastr popsán v této sekci. Další informace viz téma “Vytvoření nového uniformní klastru” na stránce 414. Při použití této funkce můžete pojmenovat dva správce front a zadat jejich názvy připojení pro úplná úložiště pro tento automatický klastr.

Následující atributy jsou volitelné pro sekci AutoCluster , ale musíte je poskytnout ve dvojicích:

NázevRepository1 =*< řetězce>*
Jedná se o název správce front pro první úplné úložiště v automatickém klastru. Může se jednat o název tohoto správce front nebo jiného správce front.

Repository1Conname=*< Řetězec názvu připojení >*
Jedná se o hodnotu názvu připojení (CONNAME) pro způsob připojení členů automatického klastru k tomuto správci front.

Dále můžete identifikovat druhé úplné úložiště pro klastr:

Repository2Name=*< String>*
Repository2Conname=*< Řetězec názvu připojení >*

Příklad sekce:

```
AutoCluster:
   Repository2Conname=myFR1.hostname(1414)
   Repository2Name=QMFR1
   Repository1Conname= myFR2.hostname(1414)
   Repository1Name=QMFR2
   ClusterName=UNICLUS
   Type=Uniform
```

Atributy pro sekci Proměnné

Dvojice `attribute=value` je platná v poli atributu. Ty lze zadat pomocí volby příkazového řádku **-iv** v příkazu **crtmqm** při vytváření správce front.

Atributy uvedené v sekci Proměnné můžete použít během automatické konfigurace klastru polí CONNAME a MQSC názvu kanálu příjemce klastru.

Pozastavení správce front z uniformního klastru

Během normálního provozu uniformního klastru mohou být znovu připojitelné instance klientské aplikace kdykoli automaticky vyváženy ke kterémukoli správci front v klastru. Chcete-li aplikacím zabránit v připojení ke konkrétnímu správci front po určitou dobu, například během operací údržby nebo určování problémů, použijte příkaz SUSPEND QMGR.

Zadejte příkaz SUSPEND QMGR CLUSTER (*jednotný název klastru*).

Kromě obvyklých účinků pozastavení v klastru IBM MQ v jednotném klastru příkaz SUSPEND také zabraňuje opětovnému vyvážení aplikací s tímto správcem front.

Všechna taková existující připojení ke správci front jsou okamžitě po zadání příkazu znovu vyvážena k ostatním dostupným správcům front v klastru.

Notes:

- Když jsou správci front pozastaveni z klastru, DIS APSTATUS je zobrazí jako AKTIVNÍ (NO), s výjimkou lokálního správce front, který vždy zobrazuje AKTIVNÍ (YES) pro svou vlastní položku stavu.
- Pokud jsou všichni správci front v jednotném klastru pozastaveni, zůstanou aplikace připojeny k jednomu nebo více pozastaveným správcům front.

Chcete-li zabránit přidávání nových připojení do udržovaného správce front, měli byste zastavit kanál připojení serveru nebo kanály používané klientskými aplikacemi, například zadáním následujícího příkazu **runmqsc** :

```
STOP CHANNEL(svrconn channel name)
```

To nemusí být možné, pokud se například tyto kanály používají také pro připojení administrativních aplikací požadovaných během okna údržby. Z tohoto důvodu pozastavený správce front pravidelně kontroluje připojené znovu připojitelné aplikace.

Jsou-li k dispozici znovu připojitelné aplikace, dojde k jejich vyvážení s ostatními dostupnými správci front v klastru. Nyní lze provádět údržbu pozastaveného správce front.

Poznámka: Aplikace, které nejsou považovány za přesunitelné, nejsou ovlivněny počátečním příkazem ani následnými opětovnými plechovkami a zůstávají připojeny k pozastavenému správci front; další podrobnosti viz MOVCOUNT .

Chcete-li obnovit pozastaveného správce front, postupujte takto:

1. V případě potřeby spusťte kanál připojení serveru a pokračujte v přijímání nových připojení aplikace zadáním následujícího příkazu:

   ```
   START CHANNEL(svrconn channel name)
   ```

2. Zadejte následující příkaz **runmqsc** :

```
RESUME QMGR CLUSTER(uniform cluster name)
```

Správce front pokračuje v komunikaci se zbytkem jednotného klastru a v případě potřeby obnovení rovnováhy jsou znovu připojitelné instance klientských aplikací přesměrovány na tohoto správce front.

Konfigurace publikování/odběru zpráv

Můžete spustit, zastavit a zobrazit stav publikování/odběru ve frontě. Můžete také přidávat a odebírat proudy a přidávat a odstraňovat správce front z hierarchie zprostředkovatele.

Procedura

- Další informace o řízení publikování/odběru ve frontě naleznete v následujících dílčích tématech:
  - “Nastavení atributů zpráv publikování/odběru ve frontě” na stránce 421
  - “Spuštění publikování/odběru ve frontě” na stránce 422
  - “Zastavení publikování/odběru ve frontě” na stránce 423
  - “Přidání proudu” na stránce 423
  - “Odstranění proudu” na stránce 424
  - “Přidání bodu odběru” na stránce 425
  - “Kombinace prostorů témat v sítích publikování/odběru” na stránce 433

Nastavení atributů zpráv publikování/odběru ve frontě

Chování některých atributů zpráv publikování/odběru můžete řídit pomocí atributů správce front. Ostatní atributy, které řídíte v sekci *Zprostředkovatel* souboru `qm.ini` .

Informace o této úloze

Můžete nastavit následující atributy publikování/odběru: podrobnosti viz Parametry správce front .

Tabulka 27. Konfigurační parametry publikování/odběru

Popis	**Název parametru MQSC**
Počet opakování zprávy příkazu	**PSRTYCNT**
Zrušit nedoručitelnou vstupní zprávu příkazu	**PSNPMSG**
Chování po zprávě s odpovědí na nedoručitelný příkaz	**PSNPRES**
Zpracovat zprávy příkazů pod synchronizačním bodem	**PSSYNCPT**

Sekce zprostředkovatele se používá ke správě následujících nastavení konfigurace:

- `PersistentPublishRetry=yes | force`

  Zadáte-li hodnotu Ano, pak pokud se publikování trvalé zprávy prostřednictvím rozhraní pro publikování/odběr ve frontě nezdaří a nebyla požadována žádná záporná odpověď, operace publikování se zopakuje.

  Pokud jste požadovali zápornou zprávu odpovědi, odešle se záporná odpověď a nedojde k žádnému dalšímu opakování.

  Zadáte-li volbu `Vynutit`, pak pokud se publikování trvalé zprávy prostřednictvím rozhraní publikování/odběru ve frontě nezdaří, operace publikování se zopakuje, dokud nebude úspěšně zpracována. Není odeslána žádná negativní odpověď.

- `NonPersistentPublishRetry= ano | vynutit`

  Zadáte-li volbu Ano, pak pokud se publikování dočasné zprávy prostřednictvím rozhraní pro publikování/odběr ve frontě nezdaří a nebyla požadována žádná záporná odpověď, operace publikování se zopakuje.

  Pokud jste požadovali zápornou zprávu odpovědi, odešle se záporná odpověď a nedojde k žádnému dalšímu opakování.

  Pokud jste zadali `Vynutit`, pak pokud se publikování dočasné zprávy prostřednictvím rozhraní pro publikování/odběr ve frontě nezdaří, operace publikování se zopakuje, dokud nebude úspěšně zpracována. Není odeslána žádná negativní odpověď.

  Poznámka: Chcete-li tuto funkci povolit pro dočasné zprávy, je třeba spolu s nastavením hodnoty `NonPersistentPublishRetry` také zajistit, aby byl atribut správce front **PSSYNCPT** nastaven na hodnotu Ano.

  To může mít také vliv na výkon zpracování dočasných publikování, protože **MQGET** z fronty STREAM se nyní vyskytuje pod synchronizačním bodem.
- `PublishBatchVelikost =`*číslo*

  Zprostředkovatel obvykle zpracovává zprávy publikování v rámci synchronizačního bodu. Může být neefektivní potvrdit každé publikování jednotlivě a za určitých okolností může zprostředkovatel zpracovat více publikačních zpráv v jedné pracovní jednotce. Tento parametr určuje maximální počet publikačních zpráv, které lze zpracovat v jedné pracovní jednotce.

  Výchozí hodnota pro `PublishBatchVelikost` je 5.
- `PublishBatchInterval =`*číslo*

  Zprostředkovatel obvykle zpracovává zprávy publikování v rámci synchronizačního bodu. Může být neefektivní potvrdit každé publikování jednotlivě a za určitých okolností může zprostředkovatel zpracovat více publikačních zpráv v jedné pracovní jednotce. Tento parametr určuje maximální dobu (v milisekundách) mezi první zprávou v dávce a následným publikováním zahrnutým ve stejné dávce.

  Interval dávky 0 označuje, že lze zpracovat až zprávy `PublishBatchSize` za předpokladu, že jsou zprávy k dispozici okamžitě.

  Výchozí hodnota pro `PublishBatchInterval` je nula.

Postup

Pomocí programu IBM MQ Explorer, programovatelných příkazů nebo příkazu **runmqsc** můžete změnit atributy správce front, které řídí chování publikování/odběru.

Příklad

ALTER QMGR PSNPRES (SAFE)

Spuštění publikování/odběru ve frontě

Publikování/odběr ve frontě spustíte nastavením atributu PSMODE správce front.

Než začnete

Přečtěte si popis PSMODE , abyste porozuměli třem režimům publikování/odběru:

- `COMPAT`
- `VYPNUTO`
- `POVOLENO`

Informace o této úloze

Nastavte atribut QMGR PSMODE tak, aby spustil buď rozhraní publikování/odběru ve frontě (známé také jako zprostředkovatel), nebo stroj publikování/odběru (také známý jako publikování/odběr verze 7), nebo obojí. Chcete-li spustit publikování/odběr ve frontě, musíte nastavit volbu PSMODE na hodnotu ENABLED. Výchozí hodnota je POVOLENO.

Postup

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

Příklad

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

Jak pokračovat dále

Produkt IBM MQ zpracovává příkazy publikování/odběru zařazené do fronty a volání rozhraní MQI (publish/subscribe Message Queue Interface).

Zastavení publikování/odběru ve frontě

Publikování/odběr ve frontě zastavíte nastavením atributu PSMODE správce front.

Než začnete

Přečtěte si popis PSMODE , abyste porozuměli třem režimům publikování/odběru:

- COMPAT
- VYPNUTO
- POVOLENO

Informace o této úloze

Nastavte atribut QMGR PSMODE tak, aby zastavil buď rozhraní publikování/odběru ve frontě (známé také jako zprostředkovatel), nebo stroj publikování/odběru (známý také jako publikování/odběr verze 7), nebo obojí. Chcete-li zastavit publikování/odběr ve frontě, musíte nastavit volbu PSMODE na hodnotu COMPAT. Chcete-li zcela zastavit stroj publikování/odběru, nastavte volbu PSMODE na hodnotu DISABLED.

Postup

Použijte příkaz IBM MQ Explorer nebo **runmqsc** k zakázání rozhraní publikování/odběru ve frontě.

Příklad

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

Přidání proudu

Proudy můžete přidat ručně, abyste povolili izolaci dat mezi aplikacemi, nebo abyste povolili vzájemnou operaci s hierarchiemi publikování/odběru produktu IBM MQ .

Než začnete

Seznamte se s tím, jak fungují proudy publikování/odběru. Viz Proudy a témata.

Informace o této úloze

K provedení těchto kroků použijte příkaz PCF, **runmqsc**nebo IBM 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 ve starší verzi produktu IBM MQ.
2. Definujte lokální téma se stejným názvem jako proud na ht dřívější verzi produktu IBM MQ.
3. Přidejte název fronty do seznamu názvů SYSTEM.QPUBSUB.QUEUE.NAMELIST .
4. Opakujte pro všechny správce front v novější verzi produktu IBM MQ , kteří jsou v hierarchii publikování/odběru.

přidání 'Sport'

V příkladu sdílení proudu 'Sport' pracují starší správci front a novější správci front IBM MQ ve stejné hierarchii publikování/odběru. Správci front starší verze sdílejí proud s názvem 'Sport'. Příklad ukazuje, jak vytvořit frontu a téma pro správce front novější verze s názvem 'Sport's řetězcem tématu 'Sport' , který je sdílen s proudem správců front dřívější verze 'Sport'.

Výsledný řetězec tématu 'Sport/Soccer/Results'vytvoří publikační aplikace správce front novější verze, která publikuje do tématu 'Sport's řetězcem tématu 'Soccer/Results'. Ve správcích front novější verze obdrží publikování odběratelé tématu 'Sport's řetězcem tématu 'Soccer/Results' .

Ve správcích front starších verzí odběratelé proudu 'Sport's řetězcem tématu 'Soccer/Results' obdrží publikování.

```
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: IBM MQ queue created.
define topic('Sport') topicstr('Sport')
     2 : define topic('Sport') topicstr('Sport')
AMQ8690: IBM MQ topic created.
alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport', 'SYSTEM.BROKER.DEFAULT.STREAM',
'SYSTEM.BROKER.ADMIN.STREAM')
     3 : alter namelist(SYSTEM.QPUBSUB.QUEUE.NAMELIST) NAMES('Sport', 'SYSTEM.BROKER.DEFAULT.STREAM',
'SYSTEM.BROKER.ADMIN.STREAM')
AMQ8551: IBM MQ namelist changed.
```

Poznámka: 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.

Každého správce front IBM MQ v hierarchii musíte nakonfigurovat ručně.

Odstranění proudu

Můžete odstranit proud ze správce front IBM MQ .

Než začnete

Před odstraněním proudu se musíte ujistit, že neexistují žádné zbývající odběry proudu, a uvést všechny aplikace, které tento proud používají, do klidového stavu. Pokud publikování pokračují v toku do odstraněného proudu, obnovení systému do čistě funkčního stavu vyžaduje velké administrativní úsilí.

Postup

1. Vyhledejte všechny připojené zprostředkovatele, kteří hostují tento proud.
2. Zrušte všechny odběry proudu u všech zprostředkovatelů.

3. Odeberte frontu (se stejným názvem jako proud) ze seznamu názvů SYSTEM.QPUBSUB.QUEUE.NAMELIST.
4. Odstraňte nebo vymažte všechny zprávy z fronty se stejným názvem jako proud.
5. Odstraňte frontu se stejným názvem jako proud.
6. Odstraňte přidružený objekt tématu.

Jak pokračovat dále

Opakujte kroky 3 až 5 pro všechny ostatní připojené správce front IBM MQ , kteří jsou hostitelem proudu.

Přidání bodu odběru

Jak rozšířit existující aplikaci publikování/odběru zařazenou ve frontě, kterou jste migrovali ze starší verze produktu IBM Integration Bus , o nový bod odběru.

Než začnete

1. Zkontrolujte, zda není bod odběru již definován v souboru SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.
2. Zkontrolujte, zda existuje objekt tématu nebo řetězec tématu se stejným názvem jako bod odběru.

Informace o této úloze

IBM MQ, aplikace nepoužívají body odběru, ale mohou spolupracovat s existujícími aplikacemi, které tak činí, pomocí mechanizmu migrace bodu odběru.

Důležité: Mechanizmus migrace bodu odběru byl odebrán z adresáře IBM MQ 8.0. Potřebujete-li migrovat existující aplikace, musíte před migrací na nejnovější verzi provést postupy popsané v dokumentaci pro vaši verzi produktu.

Není třeba přidávat body odběru pro použití integrovaných aplikací publikování/odběru napsaných pro verze produktu IBM MQ.

Postup

1. Přidejte název bodu odběru do souboru SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.
   - V systému z/OSmá parametr **NLTYPE** výchozí hodnotu NONE.
   - Zopakujte krok v každém správci front, který je připojen ve stejné topologii publikování/odběru.
2. Přidejte objekt tématu, nejlépe s názvem bodu odběru, s řetězcem tématu odpovídajícím názvu bodu odběru.
   - Pokud je bod odběru v klastru, přidejte objekt tématu jako téma klastru na hostiteli tématu klastru.
   - Pokud existuje objekt tématu se stejným řetězcem tématu jako název bodu odběru, použijte existující objekt tématu. Je třeba porozumět důsledkům opakovaného použití existujícího tématu v rámci bodu odběru. Pokud je existující téma součástí existující aplikace, musíte vyřešit kolizi mezi dvěma identicky pojmenovanými tématy.
   - Pokud existuje objekt tématu se stejným názvem jako bod odběru, ale s jiným řetězcem tématu, vytvořte téma s jiným názvem.
3. Nastavte atribut **Topic** ZÁSTUPNÝ znak na hodnotu BLOCK.

   Blokování odběrů pro # nebo * izoluje odběry se zástupnými znaky pro body odběru, viz Zástupné znaky a body odběru.
4. Nastavte všechny požadované atributy v objektu tématu.

Příklad

Příklad zobrazuje 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. Zahrňte výchozí bod odběru do seznamu bodů odběru přidaných pomocí příkazu **ALTER** . Produkt **ALTER** odstraní existující názvy ze seznamu názvů.
2. Před změnou seznamu názvů definujte témata. Správce front kontroluje seznam názvů pouze při spuštění správce front a při změně seznamu názvů.

Konfigurace distribuovaných sítí publikování/odběru

Správci front, kteří jsou navzájem propojeni do distribuované topologie publikování/odběru, sdílejí společný federovaný prostor tématu. Odběry vytvořené v jednom správci front mohou přijímat zprávy publikované aplikací připojenou k jinému správci front v topologii.

Rozsah prostorů témat vytvořených propojením správců front v klastrech nebo hierarchiích můžete řídit. V klastru publikování/odběru musí být objekt tématu 'klastrovaný' pro každou větev prostoru tématu, která má přesahovat klastr. V hierarchii musí být každý správce front nakonfigurován tak, aby identifikoval svého 'nadřízeného' v hierarchii.

Můžete dále řídit tok publikování a odběrů v rámci topologie výběrem toho, zda je každé publikování a odběr buď lokální, nebo globální. Lokální publikování a odběry nejsou šířeny mimo správce front, ke kterému je vydavatel nebo odběratel připojen.

Související pojmy

Distribuované sítě publikování/odběru

Obor publikování

Obor odběru

Prostory témat

Související úlohy

Definování témat klastru

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li nastavit téma jako téma klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikování a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Než začnete

Některé konfigurace klastru nemohou pojmout režijní náklady přímo směrovaného publikování/odběru. Před použitím této konfigurace prozkoumejte aspekty a volby uvedené v části Navrhování klastrů publikování/odběru.

Aby se změny klastru šířily v rámci klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy se ujistěte, že jsou vaše úložiště k dispozici.

Viz také téma Směrování pro klastry publikování/odběru: Poznámky k chování.

Scénář:

- Klastr INVENTORY byl nastaven podle popisu v části “Přidání správce front do klastru” na stránce 308. Obsahuje tři správce front: LONDON a NEWYORK obě obsahují úplná úložiště, PARIS obsahují dílčí úložiště.

Informace o této úloze

Při definování tématu ve správci front v klastru je třeba určit, zda se jedná o téma klastru, a pokud ano, o směrování v rámci klastru pro publikování a odběry tohoto tématu. Chcete-li nastavit téma jako téma klastru, nakonfigurujte vlastnost **CLUSTER** na objektu TOPIC s názvem klastru. Definováním tématu klastru ve správci front v klastru toto téma zpřístupníte celému klastru. Chcete-li zvolit směrování zpráv, které má být použito v rámci klastru, nastavte vlastnost **CLROUTE** v objektu TOPIC na jednu z následujících hodnot:

- **DIRECT**
- **TOPICHOST**

Standardně je směrování tématu **DIRECT**. Před produktem IBM MQ 8.0 bylo k dispozici pouze toto směrování. Pokud nakonfigurujete přímo směrované klastrované téma ve správci front, všichni správci front ve klastru budou mít informace o všech ostatních správcích front ve klastru. Při provádění operací publikování a odběru se každý správce fronty může připojit přímo k jinému správci fronty v klastru. Viz Přímo směrované klastry publikování/odběru.

Od IBM MQ 8.0můžete místo toho konfigurovat směrování témat jako **TOPICHOST**. Při použití směrování hostitelů témat budou mít všichni správci front v klastru informace o správcích front klastru, kteří jsou hostiteli směrované definice tématu (tj. správcích front, na kterých jste definovali objekt tématu). Při provádění operací publikování a odběru se správci front v klastru připojí pouze ke správcům front hostitele tématu a nikoli přímo každý s každým. Správci front hostitele tématu odpovídají za směrování publikování ze správců front, na nichž dochází k publikování publikací, na správce front s odpovídajícími odběry. Viz Klastry publikování/odběru směrované hostitelem tématu.

Poznámka: Po klastrovaném objektu tématu (prostřednictvím nastavení vlastnosti **CLUSTER**) nemůžete změnit hodnotu vlastnosti **CLROUTE** . Před změnou hodnoty musíte vyjmout objekt z klastru (vlastnost **CLUSTER** nastavit na ' '). Vyřazením tématu z klastru převedete definici tématu na lokální téma, výsledkem čehož je období, během kterého nebudou publikace doručovány do vzdálených správců front. Tuto skutečnost byste měli při provádění této změny vzít v úvahu. Viz Dopad definice neklastrového tématu pod názvem témata klastru z jiného správce front . Pokud se pokusíte změnit hodnotu vlastnosti **CLROUTE** , zatímco je klastrovaná, systém vygeneruje výjimku MQRCCF_CLROUTE_NOT_ALTERABLE .

Postup

1. Zvolte správce front, který bude hostitelem vašeho tématu.

   Téma může být hostitelem libovolného správce front klastru. Vyberte jednoho ze tří správců front (LONDON, NEWYORK nebo PARIS) a nakonfigurujte vlastnosti objektu TOPIC . Pokud plánujete používat přímé směrování, nezpůsobí to žádný provozní rozdíl, kterého správce front zvolíte. Pokud plánujete používat směrování hostitelů témat, má vybraný správce front další odpovědnost za směrování publikací. Proto pro směrování hostitelů témat zvolte správce front, který je hostován na jednom z vašich výkonnějších systémů a má dobrou síťovou konektivitu.
2. Definujte téma ve správci front.

   Chcete-li téma nastavit jako téma klastru, zadejte při definování tématu název klastru a nastavte směrování, které chcete použít pro publikování a odběry tohoto tématu. Chcete-li například vytvořit téma klastru přímého směrování ve správci front LONDON , vytvořte téma následujícím způsobem:

   ```
   DEFINE TOPIC(INVENTORY) TOPICSTR('/INVENTORY') CLUSTER(INVENTORY) CLROUTE(DIRECT)
   ```

   Definováním tématu klastru ve správci front v klastru toto téma zpřístupníte celému klastru.

   Další informace o použití produktu **CLROUTE**viz DEFINE TOPIC (CLROUTE) a Směrování pro klastry publikování/odběru: Poznámky k chování.

Výsledky

Klastr je připraven přijímat publikování a odběry pro dané téma.

Jak pokračovat dále

Pokud jste nakonfigurovali klastr publikování/odběru se směrovaným hostitelem tématu, pravděpodobně budete pro toto téma chtít přidat druhého hostitele tématu. Viz “Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat” na stránce 430.

Máte-li několik samostatných klastrů publikování/odběru, například proto, že vaše organizace je geograficky rozptýlená, možná budete chtít rozšířit některá témata klastru do všech klastrů. To lze provést připojením klastrů v hierarchii. Viz “Kombinace prostorů témat více klastrů” na stránce 434. Můžete také řídit tok publikování z jednoho klastru do druhého. Viz “Kombinace a izolace prostorů témat ve více klastrech” na stránce 436.

Související pojmy

Kombinace rozsahů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracují publikování a rozsah odběru nezávisle na určení toku publikování mezi správci front.

Kombinace prostorů témat v sítích publikování/odběru
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo hierarchii publikování/odběru. Kombinujte klastry publikování/odběru a klastry publikování/odběru s hierarchiemi.

Související úlohy

Přesunutí definice tématu klastru do jiného správce front
V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat
V klastru publikování/odběru se směrováním hostitele tématu lze ke směrování publikování na odběry použít více správců front definováním stejného objektu klastrovaného tématu v těchto správcích front. Lze jej použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Když přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete pomocí parametru **PUB** řídit, kdy se publikování začnou směrovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování/odběru
Připojte podřízeného správce front k nadřízenému správci front v hierarchii. Pokud je podřízený správce front již členem jiné hierarchie nebo klastru, pak toto připojení spojí hierarchie dohromady nebo spojí klastr s hierarchií.

Odpojení správce front od hierarchie publikování/odběru
Odpojte podřízeného správce front od nadřízeného správce front v hierarchii publikování/odběru.

Návrh klastrů publikování/odběru

Odstraňování problémů s distribuovaným publikováním/odběry

Blokování klastrovaného publikování/odběru

Přesunutí definice tématu klastru do jiného správce front

V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Informace o této úloze

V klastru můžete mít více definic stejného objektu tématu klastru. Jedná se o normální stav pro klastr směrovaný hostitelem tématu a neobvyklý stav pro klastr směrovaný přímo. Další informace viz Vícenásobné definice témat klastru se stejným názvem.

Chcete-li přesunout definici tématu klastru do jiného správce front v klastru bez přerušení toku publikování, postupujte takto. Procedura přesune definici ze správce front `QM1` do správce front `QM2`.

Postup

1. Vytvořte duplikát definice tématu klastru na QM2.

   Pro přímé směrování nastavte všechny atributy tak, aby odpovídaly definici QM1.

   Pro směrování hostitelů témat nejprve definujte nového hostitele témat jako PUB(DISABLED). To umožňuje produktu QM2 učit se o odběrech v klastru, ale nespouštět směrování publikací.
2. Počkejte na šíření informací přes klastr.

   Počkejte na předání nové definice tématu klastru správci front úplného úložiště všem správcům front v klastru. Pomocí příkazu **DISPLAY CLUSTER** zobrazte témata klastru pro každého člena klastru a zkontrolujte definici pocházející z QM2.

   V případě směrování hostitelů témat počkejte na nového hostitele témat na serveru QM2 , abyste se dozvěděli o všech odběrech. Porovnejte proxy odběry známé produktu QM2 a ty známé produktu QM1. Jedním ze způsobů zobrazení proxy odběrů ve správci front je zadání následujícího příkazu **runmqsc** :

   ```
   DISPLAY SUB(*) SUBTYPE(PROXY)
   ```
3. V případě směrování hostitelů témat předefinujte hostitele témat v systému QM2 jako PUB(ENABLED)a poté znovu definujte hostitele témat v systému QM1 jako PUB(DISABLED).

   Nyní, když se nový hostitel tématu v systému QM2 dozvěděl o všech odběrech v jiných správcích front, může hostitel tématu spustit směrování publikování.

   Použitím nastavení PUB(DISABLED) pro uvedení zpráv do klidového stavu prostřednictvím QM1se při odstraňování definice tématu klastru ujistěte, že nejsou ve vlaku žádná publikování. QM1
4. Odstraňte definici tématu klastru z QM1.

   Definici z QM1 můžete odstranit pouze v případě, že je správce front k dispozici. Jinak musíte spustit obě existující definice, dokud nebude QM1 restartován nebo vynuceně odebrán.

   Pokud QM1 zůstává dlouho nedostupný a během této doby musíte upravit klastrovanou definici tématu na QM2, je definice QM2 novější než definice QM1 , a proto obvykle převažuje.

   Pokud během tohoto období existují rozdíly mezi definicemi v systému QM1 a QM2, budou do protokolů chyb obou správců front zapisovány chyby, které vás upozorní na konfliktní definici tématu klastru.

   Pokud se QM1 nikdy nevrátí do klastru, například kvůli neočekávanému vyřazení z provozu po selhání hardwaru, můžete jako poslední možnost použít příkaz RESET CLUSTER a vynutit vysunutí správce front. Produkt **RESET CLUSTER** automaticky odstraní všechny objekty témat, jejichž hostitelem je cílový správce front.

Související pojmy

Kombinace rozsahů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracují publikování a rozsah odběru nezávisle na určení toku publikování mezi správci front.

Kombinace prostorů témat v sítích publikování/odběru
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo hierarchii publikování/odběru. Kombinujte klastry publikování/odběru a klastry publikování/odběru s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li nastavit téma jako téma klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikování a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat
V klastru publikování/odběru se směrováním hostitele tématu lze ke směrování publikování na odběry použít více správců front definováním stejného objektu klastrovaného tématu v těchto správcích front. Lze jej použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Když přidáte dalšího hostitele tématu

pro stejný objekt tématu klastru, můžete pomocí parametru **PUB** řídit, kdy se publikování začnou směrovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování/odběru
Připojte podřízeného správce front k nadřízenému správci front v hierarchii. Pokud je podřízený správce front již členem jiné hierarchie nebo klastru, pak toto připojení spojí hierarchie dohromady nebo spojí klastr s hierarchií.

Odpojení správce front od hierarchie publikování/odběru
Odpojte podřízeného správce front od nadřízeného správce front v hierarchii publikování/odběru.

Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat

V klastru publikování/odběru se směrováním hostitele tématu lze ke směrování publikování na odběry použít více správců front definováním stejného objektu klastrovaného tématu v těchto správcích front. Lze jej použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Když přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete pomocí parametru **PUB** řídit, kdy se publikování začnou směrovat přes nového hostitele tématu.

Než začnete

Definování stejného objektu tématu klastru v několika správcích front je funkčně užitečné pouze pro klastr směrovaný hostitelem tématu. Definování více odpovídajících témat v přímo směrovaném klastru nezmění jeho chování. Tato úloha se vztahuje pouze na klastry se směrovaným hostitelem tématu.

Tato úloha předpokládá, že jste si přečetli článek Vícenásobné definice témat klastru se stejným názvem, zejména následující sekce:

- Více definic tématu klastru v klastru se směrováním hostitelů témat
- Speciální zpracování pro parametr PUB

Informace o této úloze

Je-li správce front vytvořen jako hostitel směrovaného tématu, musí nejprve zjistit existenci všech souvisejících témat, která byla přihlášena k odběru v klastru. Pokud jsou publikace publikovány do těchto témat v době, kdy je přidán další hostitel tématu, a publikace je směrována na nového hostitele dříve, než se tento hostitel dozvěděl o existenci odběrů v jiných správcích front v klastru, nový hostitel tuto publikaci těmto odběrům nepředá. To způsobí, že odběry zmeškaly publikování.

Publikace nejsou směrovány prostřednictvím správců front hostitele tématu, kteří explicitně nastavili parametr **PUB** objektu tématu klastru na hodnotu `DISABLED`, takže můžete pomocí tohoto nastavení zajistit, aby během procesu přidávání dalšího hostitele tématu nechyběly žádné odběry publikací.

Poznámka: Zatímco je správce front hostitelem tématu klastru, které bylo definováno jako `PUB(DISABLED)`, vydavatelé připojení k tomuto správci front nemohou publikovat zprávy a odpovídající odběry v tomto správci front nepřijímají publikování publikovaná v jiných správcích front v klastru. Z tohoto důvodu je třeba pečlivě zvážit definování témat směrovaných hostitelem tématu ve správcích front, kde existují odběry a aplikace publikování se připojují.

Postup

1. Konfigurujte nového hostitele tématu a na počátku definujte nového hostitele tématu jako `PUB(DISABLED)`.

   To umožní novému hostiteli tématu naučit se o odběrech v klastru, ale ne spouštět směrování publikací.

   Informace o konfiguraci hostitele tématu viz “Konfigurace klastru publikování/odběru” na stránce 426.
2. Určete, kdy se nový hostitel tématu dozvěděl o všech odběrech.

Chcete-li tak učinit, porovnejte proxy odběry známé novému hostiteli tématu a odběry známé existujícímu hostiteli tématu. Jedním ze způsobů, jak zobrazit proxy odběry, je zadat následující příkaz **runmqsc** : `DISPLAY SUB(*) SUBTYPE(PROXY)`

3. Předefinujte nového hostitele tématu jako `PUB(ENABLED)`.

   Poté, co se nový hostitel tématu dozvěděl o všech odběrech v jiných správcích front, může téma spustit směrování publikací.

Související pojmy

Kombinace rozsahů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracují publikování a rozsah odběru nezávisle na určení toku publikování mezi správci front.

Kombinace prostorů témat v sítích publikování/odběru
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo hierarchii publikování/odběru. Kombinujte klastry publikování/odběru a klastry publikování/odběru s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li nastavit téma jako téma klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikování a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesunutí definice tématu klastru do jiného správce front
V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Připojení správce front k hierarchii publikování/odběru
Připojte podřízeného správce front k nadřízenému správci front v hierarchii. Pokud je podřízený správce front již členem jiné hierarchie nebo klastru, pak toto připojení spojí hierarchie dohromady nebo spojí klastr s hierarchií.

Odpojení správce front od hierarchie publikování/odběru
Odpojte podřízeného správce front od nadřízeného správce front v hierarchii publikování/odběru.

Kombinace rozsahů publikování a odběrů

Počínaje produktem IBM WebSphere MQ 7.0 pracují publikování a rozsah odběru nezávisle na určení toku publikování mezi správci front.

Publikování mohou směřovat do všech správců front, kteří jsou připojeni v topologii publikování/odběru, nebo pouze do lokálního správce front. Podobně pro proxy odběry. Publikace, které odpovídají odběru, se řídí kombinací těchto dvou toků.

Publikování a odběry lze vymezit na hodnotu `QMGR` nebo `ALL`. Jsou-li vydavatel i odběratel připojeni ke stejnému správci front, nastavení oboru neovlivní publikování, která odběratel obdrží od tohoto vydavatele.

Pokud jsou vydavatel a odběratel připojeni k různým správcům front, musí mít obě nastavení hodnotu `ALL` , aby bylo možné přijímat vzdálená publikování.

Předpokládejme, že vydavatelé jsou připojeni k různým správcům front. Chcete-li, aby odběratel přijímal publikování od libovolného vydavatele, nastavte rozsah odběru na hodnotu `ALL`. Pro každého vydavatele se pak můžete rozhodnout, zda omezit rozsah jeho publikování na odběratele, kteří jsou pro vydavatele lokální.

Předpokládejme, že odběratelé jsou připojeni k různým správcům front. Chcete-li, aby publikování od vydavatele byla odeslána všem odběratelům, nastavte rozsah publikování na hodnotu `ALL`. Chcete-li, aby odběratel přijímal publikování pouze od vydavatele připojeného ke stejnému správci front, nastavte obor odběru na hodnotu `QMGR`.

Příklad: služba fotbalových výsledků

Předpokládejme, že jste členem týmu ve fotbalové lize. Každý tým má správce front připojený ke všem ostatním týmům v klastru publikování/odběru.

Týmy zveřejňují výsledky všech zápasů hraných na domácím poli pomocí tématu `Football/result/` *`Home team name/Away team name`*. Řetězce uvedené kurzívou jsou názvy témat proměnných a publikování je výsledkem shody.

Každý klub také znovu publikuje výsledky pouze pro klub pomocí řetězce tématu `Football/myteam/` *`Home team name/Away team name`*.

Obě témata jsou publikována v celém klastru.

Následující odběry byly nastaveny ligou tak, aby fanoušci jakéhokoli týmu se mohli přihlásit k odběru výsledků třemi zajímavými způsoby.

Všimněte si, že pomocí produktu SUBSCOPE(QMGR) můžete nastavit témata klastru. Definice témat jsou šířeny do každého člena klastru, ale rozsah odběru je pouze lokální správce front. Odběratelé v každém správci front tak obdrží různá publikování ze stejného odběru.

Přijmout všechny výsledky

```
DEFINE TOPIC(A) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(ALL)
```

Získat všechny domácí výsledky

```
DEFINE TOPIC(B) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR , odpovídají pouze výsledky publikované v domovské zemi.

Získat výsledky všech mých týmů

```
DEFINE TOPIC(C) TOPICSTR('Football/myteam/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR , shodují se pouze výsledky lokálního týmu, které jsou publikovány lokálně.

Související pojmy

Kombinace prostorů témat v sítích publikování/odběru
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo hierarchii publikování/odběru. Kombinujte klastry publikování/odběru a klastry publikování/odběru s hierarchiemi.

Distribuované sítě publikování/odběru

Obor publikování

Obor odběru

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li nastavit téma jako téma klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikování a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesunutí definice tématu klastru do jiného správce front
V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat
V klastru publikování/odběru se směrováním hostitele tématu lze ke směrování publikování na odběry použít více správců front definováním stejného objektu klastrovaného tématu v těchto správcích front. Lze jej použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Když přidáte dalšího hostitele tématu

pro stejný objekt tématu klastru, můžete pomocí parametru **PUB** řídit, kdy se publikování začnou směrovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování/odběru
Připojte podřízeného správce front k nadřízenému správci front v hierarchii. Pokud je podřízený správce front již členem jiné hierarchie nebo klastru, pak toto připojení spojí hierarchie dohromady nebo spojí klastr s hierarchií.

Odpojení správce front od hierarchie publikování/odběru
Odpojte podřízeného správce front od nadřízeného správce front v hierarchii publikování/odběru.

Kombinace prostorů témat v sítích publikování/odběru

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo hierarchii publikování/odběru. Kombinujte klastry publikování/odběru a klastry publikování/odběru s hierarchiemi.

Můžete vytvořit různé prostory tématu publikování/odběru pomocí stavebních bloků atributů **CLUSTER**, **PUBSCOPE** a **SUBSCOPE** , klastrů publikování/odběru a hierarchií publikování/odběru.

Počínaje příkladem rozšiřitelnosti z jednoho správce front na klastr publikování/odběru následující scénáře ilustrují různé topologie publikování/odběru.

Související pojmy

Kombinace rozsahů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracují publikování a rozsah odběru nezávisle na určení toku publikování mezi správci front.

Distribuované sítě publikování/odběru

Prostory témat

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li nastavit téma jako téma klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikování a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesunutí definice tématu klastru do jiného správce front
V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat
V klastru publikování/odběru se směrováním hostitele tématu lze ke směrování publikování na odběry použít více správců front definováním stejného objektu klastrovaného tématu v těchto správcích front. Lze jej použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Když přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete pomocí parametru **PUB** řídit, kdy se publikování začnou směrovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování/odběru
Připojte podřízeného správce front k nadřízenému správci front v hierarchii. Pokud je podřízený správce front již členem jiné hierarchie nebo klastru, pak toto připojení spojí hierarchie dohromady nebo spojí klastr s hierarchií.

Odpojení správce front od hierarchie publikování/odběru
Odpojte podřízeného správce front od nadřízeného správce front v hierarchii publikování/odběru.

Definování témat klastru

Vytvoření jednoho prostoru tématu v klastru publikování/odběru

Rozšiřte systém publikování/odběru tak, aby se spouštěl ve více správcích front. Pomocí klastru publikování/odběru poskytněte každému vydavateli a odběrateli jeden identický prostor tématu.

Než začnete

Implementovali jste systém publikování/odběru v jednom správci front verze 7.

Vždy vytvořte prostory témat s vlastními kořenovými tématy, místo abyste se spoléhali na zdědění atributů SYSTEM.BASE.TOPIC. Pokud rozšiřujete systém publikování/odběru až na klastr, můžete definovat svá kořenová témata jako témata klastru, na hostiteli témat klastru a poté budou všechna vaše témata sdílena v rámci klastru.

Informace o této úloze

Nyní chcete systém škálovat tak, aby podporoval více vydavatelů a odběratelů a aby bylo každé téma viditelné v celém klastru.

Postup

1. Vytvořte klastr pro použití se systémem publikování/odběru.

   Máte-li existující tradiční klastr, z důvodů výkonu je lepší nastavit nový klastr pro nový systém publikování a odběru. Pro úložiště klastru obou klastrů můžete použít stejné servery.
2. Jako hostitele tématu klastru vyberte jednoho správce front, případně jedno z úložišť.
3. Ujistěte se, že každé téma, které má být viditelné v celém klastru publikování/odběru, se interpretuje jako objekt administrativního tématu.
   Nastavte atribut **CLUSTER** pojmenovávání klastru publikování/odběru.

Jak pokračovat dále

Připojte aplikace vydavatele a odběratele k libovolným správcům front v klastru.

Vytvořte objekty administrativních témat, které mají atribut **CLUSTER** . Témata jsou také šířena v rámci klastru. Programy vydavatelů a odběratelů používají administrativní témata, aby se jejich chování nezměnilo připojením k různým správcům front v klastru.

Pokud potřebujete, aby se produkt SYSTEM.BASE.TOPIC choval jako téma klastru v každém správci front, musíte jej upravit v každém správci front.

Související pojmy

Distribuované sítě publikování/odběru

Prostory témat

Související úlohy

Kombinace prostorů témat více klastrů
Vytvořte prostory tématu, které zahrnují více klastrů. Publikujte do tématu v jednom klastru a přihlaste se k jeho odběru v jiném klastru.

Kombinace a izolace prostorů témat ve více klastrech
Izolujte některé prostory témat do specifického klastru a zkombinujte ostatní prostory témat, abyste je zpřístupnili ve všech připojených klastrech.

Publikování a přihlášení k odběru prostorů témat ve více klastrech
Publikujte a odebírejte témata ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít, pokud se prostory témat v klastrech nepřekrývají.

Definování témat klastru

Kombinace prostorů témat více klastrů

Vytvořte prostory tématu, které zahrnují více klastrů. Publikujte do tématu v jednom klastru a přihlaste se k jeho odběru v jiném klastru.

Než začnete

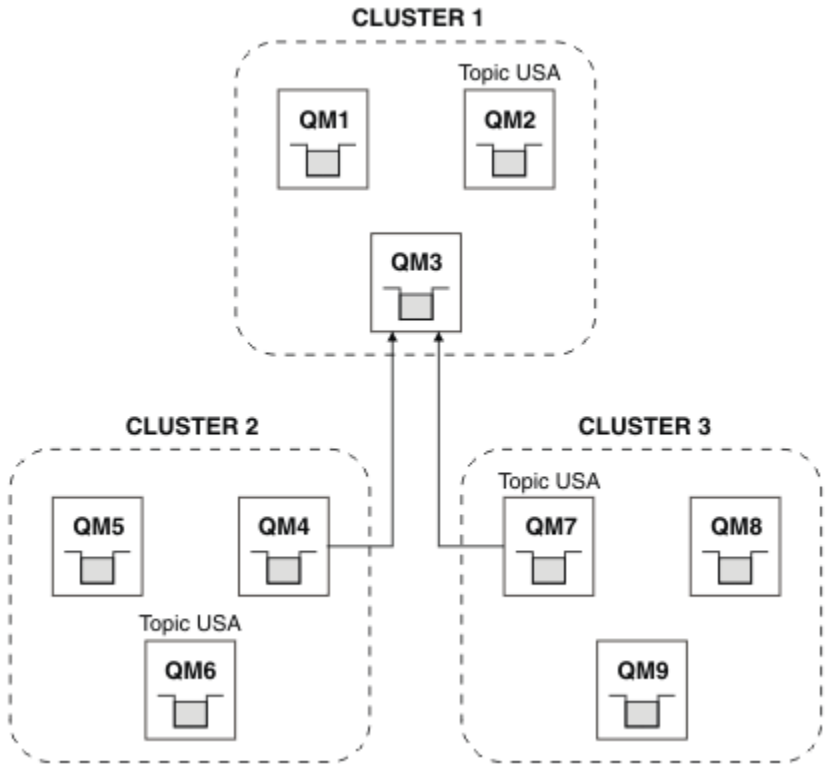
Tato úloha předpokládá, že máte existující přímo směrované klastry publikování/odběru a chcete rozšířit některá témata klastru do všech klastrů.

Poznámka: To nelze provést pro klastry publikování/odběru směrované hostitelem tématu.

Informace o této úloze

Chcete-li šířit publikace z jednoho klastru do jiného, musíte sloučit klastry dohromady v hierarchii; viz Obrázek 65 na stránce 435. Hierarchická připojení šíří odběry a publikování mezi připojenými správci front a klastry šíří témata klastrů v rámci jednotlivých klastrů, nikoli však mezi klastry.

Kombinace těchto dvou mechanizmů rozšíří témata klastru mezi všechny klastry. Je třeba opakovat definice témat klastru v každém klastru.



Obrázek 65. Připojení klastrů pomocí hierarchií

Následující kroky spojují klastry do hierarchie.

Postup

1. Vytvořte dvě sady přijímacích kanálů odesilatele pro připojení QM3 a QM4a QM3 a QM7v obou směrech. Chcete-li připojit hierarchii, musíte použít tradiční odesílací a přijímací kanály a přenosové fronty, nikoli klastr.
2. Vytvořte tři přenosové fronty s názvy cílových správců front. Aliasy správce front použijte, pokud z nějakého důvodu nemůžete použít název cílového správce front jako název přenosové fronty.
3. Nakonfigurujte přenosové fronty tak, aby spouštěli odesílací kanály.
4. Zkontrolujte, zda je parametr **PSMODE** QM3, QM4 a QM7 nastaven na hodnotu ENABLE.
5. Změňte atribut **PARENT** QM4 a QM7 na QM3.
6. Zkontrolujte, zda je stav vztahu nadřízený-podřízený mezi správci front aktivní v obou směrech.
7. Vytvořte administrativní téma USA s atributem **CLUSTER** ('CLUSTER 1'), **CLUSTER** ('CLUSTER 2') a **CLUSTER** ('CLUSTER 3'). v každém ze tří správců front hostitele tématu klastru v klastrech 1, 2 a 3. Hostitel tématu klastru nemusí být hierarchicky připojeným správcem front.

Jak pokračovat dále

Nyní můžete publikovat nebo odebírat téma klastru USA v adresáři Obrázek 65 na stránce 435. Odběry publikací směřují k vydavatelům a odběratelům ve všech třech klastrech.

Předpokládejme, že jste nevytvořili USA jako téma klastru v ostatních klastrech. Je-li parametr USA definován pouze v systému QM7, jsou publikace a odběry produktu USA vyměňovány mezi QM7, QM8, QM9a QM3. Vydavatelé a odběratelé spuštění na QM7, QM8, QM9 zdědí atributy administrativního tématu USA. Vydavatelé a odběratelé v systému QM3 zdědí atributy SYSTEM.BASE.TOPIC on QM3.

Další informace najdete v tématu “Kombinace a izolace prostorů témat ve více klastrech” na stránce 436.

Související pojmy

Distribuované sítě publikování/odběru

Prostory témat

Související úlohy

Vytvoření jednoho prostoru tématu v klastru publikování/odběru
Rozšiřte systém publikování/odběru tak, aby se spouštěl ve více správcích front. Pomocí klastru publikování/odběru poskytněte každému vydavateli a odběrateli jeden identický prostor tématu.

Kombinace a izolace prostorů témat ve více klastrech
Izolujte některé prostory témat do specifického klastru a zkombinujte ostatní prostory témat, abyste je zpřístupnili ve všech připojených klastrech.

Publikování a přihlášení k odběru prostorů témat ve více klastrech
Publikujte a odebírejte témata ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít, pokud se prostory témat v klastrech nepřekrývají.

Definování témat klastru

Kombinace a izolace prostorů témat ve více klastrech

Izolujte některé prostory témat do specifického klastru a zkombinujte ostatní prostory témat, abyste je zpřístupnili ve všech připojených klastrech.

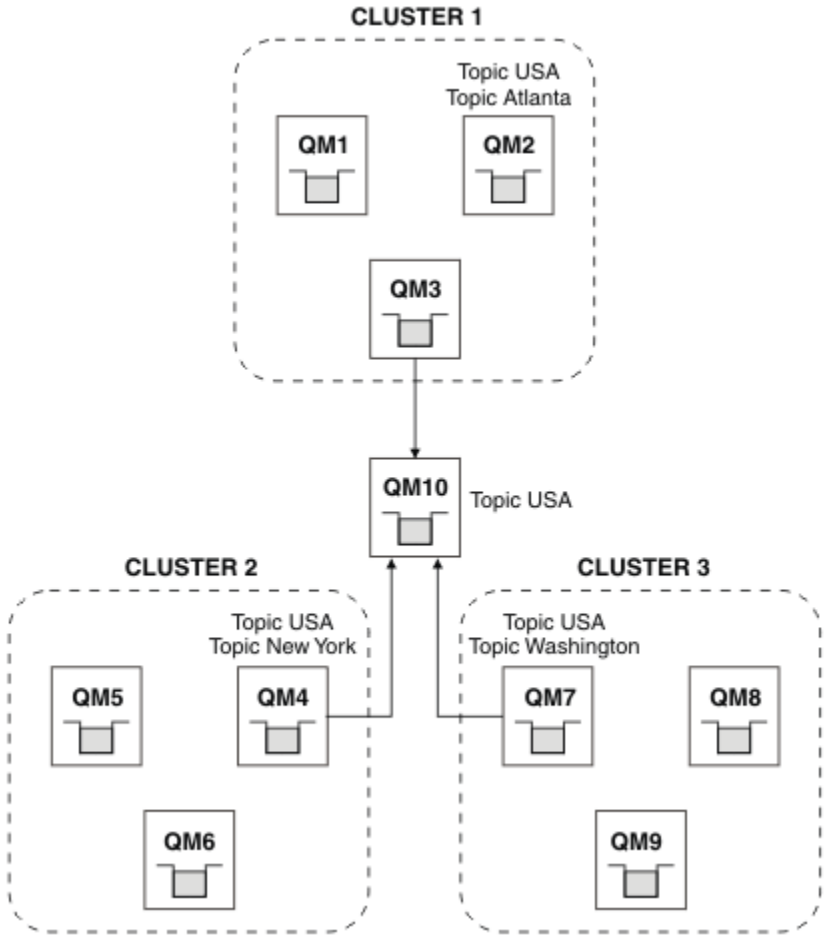
Než začnete

Prohlédněte si téma “Kombinace prostorů témat více klastrů” na stránce 434. Může být dostačující pro vaše potřeby bez přidání dalšího správce front jako mostu.

Poznámka: Tuto úlohu můžete provést pouze pomocí přímo směrovaných klastrů publikování/odběru. Tuto operaci nelze provést pomocí klastrů směrovaných hostitelem tématu.

Informace o této úloze

Potenciálním zlepšením topologie zobrazeného v souboru Obrázek 65 na stránce 435
v souboru “Kombinace prostorů témat více klastrů” na stránce 434 je izolovat témata klastru, která nejsou sdílena ve všech klastrech. Izolujte klastry vytvořením správce front přemostění, který není v žádném z klastrů; viz Obrázek 66 na stránce 437. Pomocí správce front přemostění můžete filtrovat, která publikování a odběry mohou proudit z jednoho klastru do jiného.



Obrázek 66. Přemostěné klastry

Pomocí mostu můžete izolovat témata klastru, která nechcete vystavit v rámci mostu na ostatních klastrech. V produktu Obrázek 66 na stránce 437je USA téma klastru sdílené ve všech klastrech a `Atlanta`, `New York` a `Washington` jsou témata klastru, která jsou sdílena pouze v jednom klastru.

Modelujte konfiguraci pomocí následujícího postupu:

Postup

1. Upravte všechny objekty tématu `SYSTEM.BASE.TOPIC` tak, aby měly hodnotu **SUBSCOPE** (`QMGR`). a **PUBSCOPE** (`QMGR`) ve všech správcích front.

   Žádná témata (ani témata klastru) nejsou šířena do jiných správců front, pokud explicitně nenastavíte **SUBSCOPE** (`ALL`). a **PUBSCOPE** (`ALL`) v kořenovém tématu témat klastru.
2. Definujte témata ve třech správcích front hostitele témat klastru, které chcete sdílet v každém klastru s atributy **CLUSTER** (*název_klastru*), **SUBSCOPE** (`ALL`). a **PUBSCOPE** (`ALL`).

   Chcete-li některá témata klastrů sdílet mezi všemi klastry, definujte stejné téma v každém z klastrů. Jako atribut klastru použijte název klastru každého klastru.
3. Pro témata klastru, která chcete sdílet mezi všemi klastry, definujte témata znovu ve správci front mostu (`QM10`) s atributy **SUBSCOPE** (`ALL`) a **PUBSCOPE** (`ALL`).

Příklad

V příkladu v souboru Obrázek 66 na stránce 437se mezi všemi třemi klastry šíří pouze témata, která dědí z produktu USA .

Jak pokračovat dále

Odběry pro témata definovaná ve správci front mostu s volbou **SUBSCOPE** (ALL) a **PUBSCOPE** (ALL) jsou šířeny mezi klastry.

Odběry pro témata definovaná v rámci každého klastru s atributy **CLUSTER** (*clustername*), **SUBSCOPE** (ALL) a **PUBSCOPE** (ALL) jsou šířeny v rámci každého klastru.

Všechny ostatní odběry jsou pro správce front lokální.

Související pojmy

Distribuované sítě publikování/odběru

Prostory témat

Obor publikování

Obor odběru

Související úlohy

Vytvoření jednoho prostoru tématu v klastru publikování/odběru
Rozšiřte systém publikování/odběru tak, aby se spouštěl ve více správcích front. Pomocí klastru publikování/odběru poskytněte každému vydavateli a odběrateli jeden identický prostor tématu.

Kombinace prostorů témat více klastrů
Vytvořte prostory tématu, které zahrnují více klastrů. Publikujte do tématu v jednom klastru a přihlaste se k jeho odběru v jiném klastru.

Publikování a přihlášení k odběru prostorů témat ve více klastrech
Publikujte a odebírejte témata ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít, pokud se prostory témat v klastrech nepřekrývají.

Definování témat klastru

Publikování a přihlášení k odběru prostorů témat ve více klastrech

Publikujte a odebírejte témata ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít, pokud se prostory témat v klastrech nepřekrývají.

Než začnete

Vytvořte více tradičních klastrů s některými správci front v průsečících mezi klastry.

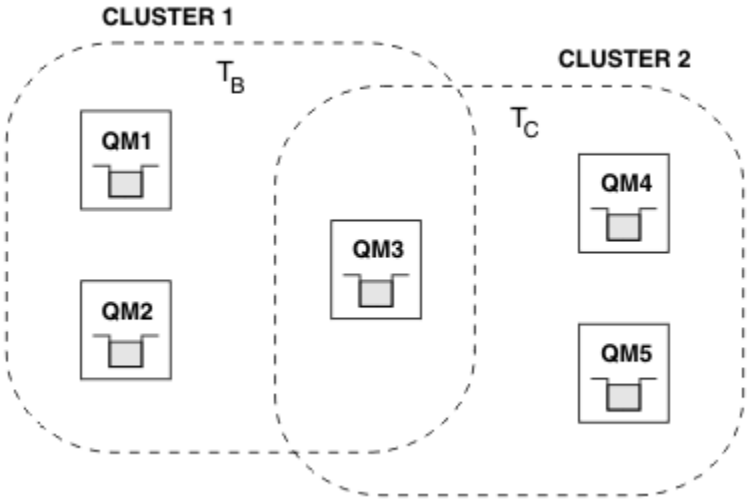
Informace o této úloze

Možná jste se rozhodli překrývat klastry z různých důvodů.

1. Máte omezený počet serverů s vysokou dostupností nebo správců front. Rozhodnete se implementovat všechna úložiště klastru a hostitele témat klastru.
2. Máte existující tradiční klastry správců front, které jsou připojeny pomocí správců front brány. Chcete implementovat aplikace publikování/odběru do stejné topologie klastru.
3. Máte několik samostatně obsažených aplikací publikování/odběru. Z výkonnostních důvodů je lepší udržovat klastry publikování/odběru malé a oddělené od tradičních klastrů. Rozhodli jste se implementovat aplikace do různých klastrů. Chcete však také monitorovat všechny aplikace publikování/odběru v jednom správci front, protože jste licencovali pouze jednu kopii aplikace monitorování. Tento správce front musí mít přístup k publikacím témat klastru ve všech klastrech.

Zajistíte-li, že vaše témata budou definována v nepřekrývajících se prostorech témat, můžete je implementovat do překrývajících se klastrů publikování/odběru, viz Obrázek 67 na stránce 439. Pokud se prostory témat překrývají, pak implementace do překrývajících se klastrů vede k problémům.

Vzhledem k tomu, že se klastry publikování/odběru překrývají, můžete publikovat a odebírat libovolný z prostorů témat pomocí správců front v překrývání.



Obrázek 67. Překrývající se klastry, nepřekrývající se prostory tématu

Postup

Vytvořte způsob, jak zajistit, aby se prostory tématu nepřekrývaly.

Například definujte jedinečné kořenové téma pro každý z prostorů témat. Vytvořte témata klastru kořenových témat.

a) `DEFINE TOPIC(B) TOPICSTR('B') CLUSTER('CLUSTER 1') ...`

b) `DEFINE TOPIC(C) TOPICSTR('C') CLUSTER('CLUSTER 2') ...`

Příklad

V produktu Obrázek 67 na stránce 439 mohou vydavatelé a odběratel připojení k produktu QM3 publikovat nebo odebírat produkt T_B nebo T_C.

Jak pokračovat dále

Připojte vydavatele a odběratele, kteří používají témata v obou klastrech, ke správcům front v překryvu.

Připojte vydavatele a odběratele, kteří musí používat pouze témata ve specifickém klastru, ke správcům front, kteří se nepřekrývají.

Související pojmy

Distribuované sítě publikování/odběru

Prostory témat

Související úlohy

Vytvoření jednoho prostoru tématu v klastru publikování/odběru
Rozšiřte systém publikování/odběru tak, aby se spouštěl ve více správcích front. Pomocí klastru publikování/odběru poskytněte každému vydavateli a odběrateli jeden identický prostor tématu.

Kombinace prostorů témat více klastrů
Vytvořte prostory tématu, které zahrnují více klastrů. Publikujte do tématu v jednom klastru a přihlaste se k jeho odběru v jiném klastru.

Kombinace a izolace prostorů témat ve více klastrech
Izolujte některé prostory témat do specifického klastru a zkombinujte ostatní prostory témat, abyste je zpřístupnili ve všech připojených klastrech.

Definování témat klastru

Připojení správce front k hierarchii publikování/odběru

Připojte podřízeného správce front k nadřízenému správci front v hierarchii. Pokud je podřízený správce front již členem jiné hierarchie nebo klastru, pak toto připojení spojí hierarchie dohromady nebo spojí klastr s hierarchií.

Než začnete

1. Správci front v hierarchii publikování/odběru musí mít jedinečné názvy správců front.
2. Hierarchie publikování/odběru spoléhá na funkci správce front "publikování/odběr ve frontě" . Tato volba musí být povolena v nadřízených i podřízených správcích front. Viz “Spuštění publikování/odběru ve frontě” na stránce 422.
3. Vztah publikování/odběru závisí na kanálech odesilatele a příjemce správce front. Existují dva způsoby, jak vytvořit kanály:
   - Přidejte nadřízeného i podřízeného správce front do klastru IBM MQ . Viz téma “Přidání správce front do klastru” na stránce 308.
   - Vytvořte dvojici odesílacího a přijímacího kanálu z podřízeného správce front do nadřízeného a z nadřízeného do podřízeného. Každý kanál musí buď používat přenosovou frontu se stejným názvem jako cílový správce front, nebo alias správce front se stejným názvem jako cílový správce front. Další informace o tom, jak vytvořit připojení kanálu dvoubodového spojení, viz “IBM MQ techniky distribuovaného řazení do front” na stránce 190.

   Příklady, které konfigurují hierarchii pro každý typ konfigurace kanálu, viz následující sada scénářů hierarchie publikování/odběru:

   - Scénář 1: Použití kanálů dvoubodového spojení s aliasem názvu správce front
   - Scénář 2: Použití kanálů dvoubodového spojení se stejným názvem pro přenosovou frontu a vzdáleného správce front
   - Scénář 3: Použití kanálu klastru k přidání správce front

Informace o této úloze

Pomocí příkazu ALTER QMGR PARENT (*PARENT_NAME*) **runmqsc** připojte podřízené prvky k nadřízených prvkům. Tato konfigurace se provádí na podřízeném správci front, kde *PARENT_NAME* je název nadřízeného správce front.

Postup

ALTER QMGR PARENT (*PARENT_NAME*)

Příklad

První příklad ukazuje, jak připojit správce front QM2 jako podřízený prvek QM1, a poté se dotazovat QM2 a potvrdit, že se úspěšně stal podřízeným s **STATUS** AKTIVNÍ:

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

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)
```

Pokud se produkt **STATUS** nezobrazuje jako AKTIVNÍ, zkontrolujte, zda jsou kanály mezi podřízeným a nadřízeným správně nakonfigurovány a spuštěny. Možné chyby naleznete v obou protokolech chyb správce front.

Jak pokračovat dále

Standardně jsou témata používaná vydavateli a odběrateli v jednom správci front sdílena s vydavateli a odběrateli v ostatních správcích front v hierarchii. Spravovaná témata lze konfigurovat tak, aby řídila úroveň sdílení pomocí vlastností tématu **SUBSCOPE** a **PUBSCOPE** . Viz téma “Konfigurace distribuovaných sítí publikování/odběru” na stránce 426.

Související pojmy

Kombinace rozsahů publikování a odběrů

Počínaje produktem IBM WebSphere MQ 7.0 pracují publikování a rozsah odběru nezávisle na určení toku publikování mezi správci front.

Kombinace prostorů témat v sítích publikování/odběru

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo hierarchii publikování/odběru. Kombinujte klastry publikování/odběru a klastry publikování/odběru s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li nastavit téma jako téma klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikování a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesunutí definice tématu klastru do jiného správce front

V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat

V klastru publikování/odběru se směrováním hostitele tématu lze ke směrování publikování na odběry použít více správců front definováním stejného objektu klastrovaného tématu v těchto správcích front. Lze jej použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Když přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete pomocí parametru **PUB** řídit, kdy se publikování začnou směrovat přes nového hostitele tématu.

Odpojení správce front od hierarchie publikování/odběru

Odpojte podřízeného správce front od nadřízeného správce front v hierarchii publikování/odběru.

Související odkazy

Proudy a témata

ZOBRAZIT PUBSUB

Systém zpráv publikování/odběru

Odpojení správce front od hierarchie publikování/odběru

Odpojte podřízeného správce front od nadřízeného správce front v hierarchii publikování/odběru.

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: IBM MQ queue manager changed.
    2 : display pubsub type(child)
AMQ8147: IBM MQ object  not found.
display pubsub type(parent)
    3 : display pubsub type(parent)
AMQ8147: IBM MQ object not found.
```

Jak pokračovat dále

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

Související pojmy

Kombinace rozsahů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracují publikování a rozsah odběru nezávisle na určení toku publikování mezi správci front.

Kombinace prostorů témat v sítích publikování/odběru
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo hierarchii publikování/odběru. Kombinujte klastry publikování/odběru a klastry publikování/odběru s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li nastavit téma jako téma klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikování a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesunutí definice tématu klastru do jiného správce front
V případě klastrů směrovaných hostitelem témat nebo přímo směrovaných klastrů může být nutné při vyřazování správce front z provozu přesunout definici tématu klastru, nebo protože správce front klastru selhal nebo je po dlouhou dobu nedostupný.

Přidání dalších hostitelů témat do klastru se směrovaným hostitelem témat
V klastru publikování/odběru se směrováním hostitele tématu lze ke směrování publikování na odběry použít více správců front definováním stejného objektu klastrovaného tématu v těchto správcích front. Lze jej použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Když přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete pomocí parametru **PUB** řídit, kdy se publikování začnou směrovat přes nového hostitele tématu.

Připojení správce front k hierarchii publikování/odběru
Připojte podřízeného správce front k nadřízenému správci front v hierarchii. Pokud je podřízený správce front již členem jiné hierarchie nebo klastru, pak toto připojení spojí hierarchie dohromady nebo spojí klastr s hierarchií.

ALW Konfigurace více instalací

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

Informace o této úloze

Tyto informace platí pro AIX, Linux, and Windows.

Procedura

- Informace v následujících odkazech použijte ke konfiguraci instalací:
  - “Změna primární instalace” na stránce 450
  - “Přidružení správce front k instalaci” na stránce 451
  - “Připojení aplikací v prostředí s více instalačními prostředi” na stránce 443

ALW Připojení aplikací v prostředí s více instalačními prostředi

Pokud jsou na systémech AIX, Linux, and Windows zavedeny knihovny IBM MQ , produkt IBM MQ automaticky použije příslušné knihovny, aniž byste museli provést další akce. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Následující koncepty se používají k vysvětlení způsobu, jakým se aplikace připojují k produktu IBM MQ:

propojení
Když je aplikace kompilována, je propojena s knihovnami IBM MQ , aby se získal export funkcí, který je načten při spuštění aplikace.

Načítání
Při spuštění aplikace jsou knihovny IBM MQ umístěny a načteny. Specifický mechanizmus používaný k vyhledání knihoven se liší v závislosti na operačním systému a způsobu sestavení aplikace. Další informace o tom, jak vyhledat a načíst knihovny ve více instalačních prostředích, viz “Načítání knihoven IBM MQ” na stránce 444.

Připojování
Když se aplikace připojí ke spuštěnému správci front, například pomocí volání `MQCONN` nebo `MQCONNX` , připojí se pomocí načtených knihoven IBM MQ .

Když se serverová aplikace připojí ke správci front, musí načtené knihovny pocházet z instalace přidružené ke správci front. U více instalací v systému toto omezení přináší nové výzvy při výběru mechanizmu, který operační systém používá k vyhledání knihoven IBM MQ , které se mají načíst:

- Při použití příkazu **setmqm** ke změně instalace přidružené ke správci front se změní knihovny, které je třeba načíst.
- Když se aplikace připojuje k více správcům front vlastněným různými instalacemi, je třeba načíst více sad knihoven.

Avšak pokud jsou knihovny IBM MQ, knihovny, umístěny a načteny, IBM MQ pak načte a použije příslušné knihovny, aniž byste museli provést další akci. Když se aplikace připojí ke správci front, produkt IBM MQ načte knihovny z instalace, ke které je správce front přidružen.

Scénáře migrace a připojení aplikací s více instalacemi jsou podrobněji popsány v tématu Koexistence správce front pro více instalací v produktu AIX, Linux, and Windows.

Další informace o tom, jak načíst knihovny IBM MQ , viz “Načítání knihoven IBM MQ” na stránce 444.

Podpora a omezení

Pokud jsou vyhledány a načteny některé z následujících knihoven IBM MQ , může produkt automaticky načíst a použít příslušné knihovny:

- Knihovny serveru C
- Knihovny serveru C++
- Knihovny serveru XA
- Knihovny serveru COBOL

- Knihovny serveru COM +
- .NET v nespravovaném režimu

Produkt IBM MQ také automaticky načítá a používá příslušné knihovny pro aplikace Java a JMS v režimu vazeb.

Existuje řada omezení pro aplikace, které používají více instalací. Další informace viz “Omezení pro aplikace používající více instalací” na stránce 447.

Související pojmy

“Omezení pro aplikace používající více instalací” na stránce 447
Existují omezení při použití knihoven serveru CICS , připojení rychlých cest, popisovačů zpráv a ukončení v prostředí s více instalačními programy.

“Načítání knihoven IBM MQ” na stránce 444
Při rozhodování o tom, jak načíst knihovny IBM MQ , musíte zvážit řadu faktorů, včetně: vašeho prostředí, zda můžete změnit existující aplikace, zda chcete primární instalaci, kde je nainstalován produkt IBM MQ a zda je pravděpodobné, že se změní umístění produktu IBM MQ .

Související úlohy

Výběr primární instalace

“Změna primární instalace” na stránce 450
Příkaz **setmqinst** můžete použít k nastavení nebo zrušení nastavení instalace jako primární instalace.

“Přidružení správce front k instalaci” na stránce 451
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému AIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

ALW Načítání knihoven IBM MQ

Při rozhodování o tom, jak načíst knihovny IBM MQ , musíte zvážit řadu faktorů, včetně: vašeho prostředí, zda můžete změnit existující aplikace, zda chcete primární instalaci, kde je nainstalován produkt IBM MQ a zda je pravděpodobné, že se změní umístění produktu IBM MQ .

Způsob umístění a načtení knihoven IBM MQ závisí na vašem instalačním prostředí:

- Pokud je na systémech AIX and Linux instalována kopie verze IBM MQve výchozím umístění, existující aplikace budou i nadále pracovat stejným způsobem jako předchozí verze. Pokud však aplikace v produktu `/usr/lib`vyžadují symbolické odkazy, musíte buď vybrat instalaci verze produktu IBM MQ jako primární instalaci, nebo symbolické odkazy vytvořit ručně.
- Pokud je produkt IBM MQ nainstalován v jiném než výchozím umístění, možná budete muset změnit existující aplikace tak, aby byly načteny správné knihovny.

Způsob, jakým lze knihovny produktu IBM MQ vyhledat a načíst, závisí také na tom, jak jsou nastaveny existující aplikace pro načítání knihoven. Další informace o tom, jak lze načíst knihovny, viz “Mechanismy zavádění knihoven operačního systému” na stránce 446.

Optimálně byste měli zajistit, aby knihovna IBM MQ , kterou načítá operační systém, byla ta, ke které je správce front přidružen.

Metody pro načítání knihoven IBM MQ se liší podle platformy a každá metoda má výhody a nevýhody.

Tabulka 28. Výhody a nevýhody voleb pro načítání knihoven

Platforma	Volba	Benefity	Nevýhody
Linux AIX AIX and Linux systémy	Nastavte nebo změňte vloženou běhovou vyhledávací cestu (RPath) aplikace. Tato volba vyžaduje opětovnou kompilaci a propojení aplikace. Další informace o kompilaci a propojování aplikací naleznete v tématu Sestavení procedurální aplikace.	• Rozsah změny je jasný.	• Musíte být schopni znovu zkompilovat a propojit aplikaci. • Pokud se změní umístění IBM MQ , musíte změnit RPath.
Systémy AIX and Linux	Nastavte proměnnou prostředí *LD_LIBRARY_PATH* pomocí příkazu setmqenvnebo crtmqenvs volbou **-k** nebo **-1** . (AIX V systému AIXje tato proměnná prostředí *LIBPATH*	• Nejsou vyžadovány žádné změny existujících aplikací. • Přepíše vložené RPaths v aplikaci. • Snadno změnit proměnnou, pokud se změní umístění IBM MQ .	• Aplikace `setuid` a `setgid` nebo aplikace sestavené jinými způsoby mohou z bezpečnostních důvodů ignorovat *LD_LIBRARY_PATH* . • Specifické prostředí, takže musí být nastaveno v každém prostředí, kde je aplikace spuštěna. • Možný dopad na jiné aplikace, které spoléhají na *LD_LIBRARY_PATH*. • Linux: Kompilátor použitý k sestavení aplikace může zakázat použití proměnné *LD_LIBRARY_PATH*. Další informace naleznete v tématu Aspekty odkazování za běhu pro produkt Linux .
Windows Windows systémy	Nastavte proměnnou PATH pomocí příkazu setmqenvnebo crtmqenv.	• Pro existující aplikace nejsou vyžadovány žádné změny. • Snadno změnit proměnnou, pokud se změní umístění IBM MQ .	• Specifické prostředí, takže musí být nastaveno v každém prostředí, kde je aplikace spuštěna. • Možný dopad na jiné aplikace.

Tabulka 28. Výhody a nevýhody voleb pro načítání knihoven (pokračování)			
Platforma	**Volba**	**Benefity**	**Nevýhody**
ALW AIX, Linux, and Windows systémy	Nastavte primární instalaci na IBM MQnebo pozdější instalaci. Viz téma “Změna primární instalace” na stránce 450. Další informace o primární instalaci naleznete v tématu Výběr primární instalace.	• Pro existující aplikace nejsou vyžadovány žádné změny. • Snadná změna primární instalace, pokud se změní umístění IBM MQ . • Poskytuje podobné chování jako předchozí verze produktu IBM MQ.	• Linux AIX AIX and Linux: Nefunguje, pokud `/usr/lib` není ve výchozí vyhledávací cestě.

Aspekty načítání knihovny pro Linux

Linux

Aplikace kompilované pomocí některých verzí gcc, například verze 3.2.x, mohou mít vloženou cestu RPath, kterou nelze přepsat pomocí proměnné prostředí *LD_LIBRARY_PATH* . Pomocí příkazu `readelf -d` *`applicationName`* můžete určit, zda je aplikace ovlivněna. RPath nelze přepsat, pokud je přítomen symbol RPATH a není přítomen symbol RUNPATH.

Mechanismy zavádění knihoven operačního systému

Na systémech Windows se prohledává několik adresářů, aby se vyhledaly knihovny:

- Adresář, ze kterého je aplikace načtena.
- Aktuální adresář.
- Adresáře v proměnné prostředí *PATH* , globální proměnné *PATH* i proměnné *PATH* aktuálního uživatele.

Linux AIX Na systémech AIX and Linux existuje řada metod, které mohly být použity k vyhledání knihoven k načtení:

- Použití proměnné prostředí *LD_LIBRARY_PATH* (také *LIBPATH* v systému AIX). Je-li tato proměnná nastavena, definuje sadu adresářů, které jsou prohledávány pro požadované knihovny IBM MQ . Pokud jsou v těchto adresářích nalezeny nějaké knihovny, použijí se přednostně pro všechny knihovny, které by mohly být nalezeny pomocí jiných metod.
- Použití vložené vyhledávací cesty (RPath). Aplikace může obsahovat sadu adresářů pro vyhledávání knihoven IBM MQ . Není-li proměnná *LD_LIBRARY_PATH* nastavena nebo nebyly-li pomocí této proměnné nalezeny požadované knihovny, vyhledají se knihovny v cestě RPath. Pokud vaše existující aplikace používají cestu RPath, ale nemůžete ji znovu zkompilovat a propojit, musíte buď nainstalovat produkt IBM MQ ve výchozím umístění, nebo použít jinou metodu k vyhledání knihoven.
- Použije se výchozí cesta ke knihovně. Pokud nejsou knihovny IBM MQ nalezeny po vyhledání proměnné *LD_LIBRARY_PATH* a umístění RPath, prohledá se výchozí cesta ke knihovně. Tato cesta obvykle obsahuje `/usr/lib` nebo `/usr/lib64`. Nejsou-li knihovny nalezeny po vyhledání výchozí cesty ke knihovně, aplikace se nespustí kvůli chybějícím závislostem.

Pomocí mechanizmů operačního systému můžete zjistit, zda vaše aplikace mají vestavěnou vyhledávací cestu. Příklad:

- AIX AIX: **dump**
- Linux Linux: **`readelf`**

Související pojmy

“Omezení pro aplikace používající více instalací” na stránce 447

Existují omezení při použití knihoven serveru CICS , připojení rychlých cest, popisovačů zpráv a ukončení v prostředí s více instalačními programy.

“Připojení aplikací v prostředí s více instalačními prostředi” na stránce 443
Pokud jsou na systémech AIX, Linux, and Windows zavedeny knihovny IBM MQ , produkt IBM MQ automaticky použije příslušné knihovny, aniž byste museli provést další akce. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Související úlohy

Výběr primární instalace

“Změna primární instalace” na stránce 450
Příkaz **setmqinst** můžete použít k nastavení nebo zrušení nastavení instalace jako primární instalace.

“Přidružení správce front k instalaci” na stránce 451
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému AIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

ALW Omezení pro aplikace používající více instalací

Existují omezení při použití knihoven serveru CICS , připojení rychlých cest, popisovačů zpráv a ukončení v prostředí s více instalačními programy.

Knihovny serveru CICS

Používáte-li knihovny serveru CICS , produkt IBM MQ automaticky nevybere správnou úroveň knihovny. Musíte zkompilovat a propojit aplikace s příslušnou úrovní knihovny pro správce front, ke kterému se aplikace připojuje. Další informace viz Sestavení knihoven pro použití s produktem TXSeries for Multiplatforms verze 5.

Popisovače zpráv

Obslužné rutiny zpráv, které používají speciální hodnotu MQHC_UNASSOCIATED_HCONN , jsou omezeny na použití s první instalací zavedenou v procesu. Pokud popisovač zprávy nemůže být použit konkrétní instalací, vrátí se kód příčiny MQRC_HMSG_NOT_AVAILABLE .

Toto omezení ovlivňuje vlastnosti zprávy. Manipulátory zpráv nelze použít k získání vlastností zpráv ze správce front v jedné instalaci a jejich vložení do správce front v jiné instalaci. Další informace o popisovači zpráv naleznete v tématu MQCRTMH-Vytvoření popisovače zprávy.

Uživatelské procedury

V prostředí s více instalacemi musí být existující uživatelské procedury aktualizovány pro použití s instalacemi produktu IBM MQ . Uživatelské procedury pro převod dat generované pomocí příkazu **crtmqcvx** musí být znovu vygenerovány pomocí aktualizovaného příkazu.

Všechny uživatelské procedury musí být zapsány pomocí struktury MQIEP , nemohou používat vložený RPATH k vyhledání knihoven IBM MQ a nemohou odkazovat na knihovny IBM MQ . Další informace naleznete v tématu Zápis uživatelských procedur a instalovatelných služeb na webu AIX, Linux, and Windows .

Rychlý způsob

Na serveru s více instalacemi musí aplikace používající rychlé připojení k produktu IBM MQ dodržovat tato pravidla:

1. Správce front musí být přidružen ke stejné instalaci jako ten, ze kterého aplikace načetla běhové knihovny IBM 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 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 nerychlé cesty ke správci front přidruženému k instalaci produktu IBM MQ nemá žádný vliv na to, zda se aplikace může připojit k rychlé cestě.

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 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-Správce front Connect (rozšířený)

Struktura MQIEP

2583 (0A17) (RC2583): MQRC_INSTALLATION_MISMATCH

2587 (0A1B) (RC2587): MQRC_HMSG_NOT_AVAILABLE

2590 (0A1E) (RC2590): MQRC_FASTPATH_NOT_AVAILABLE

ALW Připojení aplikací .NET v prostředí s více instalačními systémy

Standardně aplikace používají sestavení .NET z primární instalace. Pokud neexistuje žádná primární instalace nebo pokud nechcete použít primární instalační sestavení, musíte aktualizovat konfigurační soubor aplikace nebo proměnnou prostředí *DEVPATH* .

Pokud je v systému primární instalace, jsou sestavení .NET a soubory zásad této instalace registrovány v globální mezipaměti sestavení (GAC). Sestavení .NET pro všechny ostatní instalace lze nalézt v instalační cestě každé instalace, ale sestavení nejsou registrována v GAC. Proto jsou aplikace standardně spouštěny pomocí sestavení .NET z primární instalace. Musíte aktualizovat konfigurační soubor aplikace, pokud platí některý z následujících případů:

- Nemáte primární instalaci.
- Nechcete, aby aplikace používala primární instalační sestavy.
- Primární instalace je nižší verzí produktu IBM MQ než verze, se kterou byla aplikace kompilována.

Chcete-li získat informace o tom, jak aktualizovat konfigurační soubor aplikace, prohlédněte si téma “Připojení aplikací .NET pomocí konfiguračního souboru aplikace” na stránce 448.

Musíte aktualizovat proměnnou prostředí *DEVPATH* , pokud je následující případ pravdivý:

- Chcete, aby vaše aplikace používala sestavení z neprimární instalace, ale primární instalace má stejnou verzi jako neprimární instalace.

Další informace o aktualizaci proměnné *DEVPATH* viz “Připojení aplikací .NET pomocí DEVPATH” na stránce 449.

Připojení aplikací .NET pomocí konfiguračního souboru aplikace

V konfiguračním souboru aplikace musíte nastavit různé značky tak, aby přesměrovaly aplikace tak, aby používaly sestavení, která nejsou z primární instalace.

Následující tabulka zobrazuje specifické změny, které je třeba provést v konfiguračním souboru aplikace, aby se aplikace .NET mohly připojovat pomocí konkrétních sestavení:

Tabulka 29. Konfigurace aplikací pro použití konkrétních sestavení

	Aplikace zkompilované s dřívější verzí produktu IBM MQ	**Aplikace zkompilované s novější verzí produktu IBM MQ**
Chcete-li spustit aplikaci s novější verzí primární instalace IBM MQ . (novější verze sestav v GAC):	Nejsou nutné žádné změny	Nejsou nutné žádné změny
Chcete-li spustit aplikaci s primární instalací starší verze IBM MQ . (dřívější verze sestavení v GAC):	Nejsou nutné žádné změny	V konfiguračním souboru aplikace: • Pomocí značky *bindingRedirect* můžete označit použití dřívější verze sestavení, která jsou v GAC.
Chcete-li spustit aplikaci s novější verzí neprimární instalace produktu IBM MQ . (novější verze sestavení v instalační složce):	V konfiguračním souboru aplikace: • Pomocí značky *codebase* ukažte na umístění sestavení novější verze • Pomocí značky *bindingRedirect* můžete označit použití sestavení novější verze.	V konfiguračním souboru aplikace: • Pomocí značky *codebase* ukažte na umístění sestavení novější verze
Chcete-li spustit aplikaci s dřívější verzí neprimární instalace produktu IBM MQ . (dřívější verze sestavení v instalační složce):	V konfiguračním souboru aplikace: • Pomocí značky *codebase* ukažte na umístění dřívějších sestavení verze • Zahrnout značku *publisherpolicy Apply=no*	V konfiguračním souboru aplikace: • Pomocí značky *codebase* ukažte na umístění dřívějších sestavení verze • Pomocí značky *bindingRedirect* můžete označit použití dřívějších sestavení verze. • Zahrnout značku *publisherpolicy Apply=no*

Ukázkový konfigurační soubor aplikace `NonPrimaryRedirect.config` se dodává ve složce *MQ_INSTALLATION_PATH*`\tools\dotnet\samples\base`. Tento soubor lze upravit pomocí instalační cesty IBM MQ jakékoli neprimární instalace. Soubor lze také přímo zahrnout do jiných konfiguračních souborů pomocí značky *linkedConfiguration* . Ukázky jsou k dispozici pro `nmqsget.exe.config` a `nmqsput.exe.config`. Obě ukázky používají značku *linkedConfiguration* a zahrnují soubor `NonPrimaryRedirect.config` .

Připojení aplikací .NET pomocí DEVPATH

Sestavení můžete najít pomocí proměnné prostředí *DEVPATH* . Sestavení určená proměnnou *DEVPATH* se používají přednostně před sestavením v GAC. Další informace o tom, kdy použít tuto proměnnou, naleznete v příslušné dokumentaci Microsoft k položce *DEVPATH* .

Chcete-li vyhledat sestavení pomocí proměnné prostředí *DEVPATH* , musíte nastavit proměnnou *DEVPATH* na složku, která obsahuje sestavení, která chcete použít. Poté musíte aktualizovat konfigurační soubor aplikace a přidat následující informace o konfiguraci běhového prostředí:

```
<configuration>
<runtime>
<developmentMode developerInstallation="true" />
</runtime>
</configuration>
```

Související pojmy

“Připojení aplikací v prostředí s více instalačními prostředi” na stránce 443
Pokud jsou na systémech AIX, Linux, and Windows zavedeny knihovny IBM MQ , produkt IBM MQ automaticky použije příslušné knihovny, aniž byste museli provést další akce. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Více instalací

Související úlohy

Výběr primární instalace

Použití produktu .NET

ALW Změna primární instalace

Příkaz **setmqinst** můžete použít k nastavení nebo zrušení nastavení instalace jako primární instalace.

Informace o této úloze

Tato úloha platí pro AIX, Linux, and Windows.

Primární instalace je instalace, na kterou se vztahují požadovaná umístění v rámci celého systému. Další informace o primární instalaci a pokyny pro výběr primární instalace naleznete v tématu Výběr primární instalace.

Windows Během procesu instalace v systému Windowsmůžete určit, že instalace má být primární instalací.

Linux AIX Na systémech AIX and Linux musíte po instalaci zadat příkaz **setmqinst** , abyste nastavili instalaci jako primární instalaci.

Procedura

- Chcete-li nastavit instalaci jako primární instalaci, postupujte takto:
  a) Zkontrolujte, zda je instalace již primární instalací, zadáním následujícího příkazu:

     ```
     MQ_INSTALLATION_PATH/bin/dspmqinst
     ```

     kde *MQ_INSTALLATION_PATH* je instalační cesta instalace produktu IBM MQ .
  b) Pokud je existující instalace produktu IBM MQ nastavena jako primární instalace, zrušte její nastavení , než budete pokračovat dalším krokem.
  c) Ujistěte se, že jste přihlášeni s příslušným oprávněním:
     – Linux AIX Jako root na AIX and Linux.
     – Windows Jako člen skupiny administrátorů na systémech Windows .
  d) Zadejte jeden z následujících příkazů:
     – Chcete-li nastavit primární instalaci pomocí cesty k instalaci, kterou chcete mít jako primární instalaci, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -i -p MQ_INSTALLATION_PATH
```

– Chcete-li nastavit primární instalaci pomocí názvu instalace, která má být primární instalací, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -i -n installationName
```

e) Windows
Na systémech Windows restartujte systém.

- Chcete-li zrušit nastavení instalace jako primární instalace, postupujte takto:
  a) Zkontrolujte, která instalace je primární instalací, zadáním následujícího příkazu:

```
MQ_INSTALLATION_PATH/bin/dspmqinst
```

kde *MQ_INSTALLATION_PATH* je instalační cesta instalace produktu IBM MQ .

b) Ujistěte se, že jste přihlášeni s příslušným oprávněním:

– Linux AIX Jako root na AIX and Linux.

– Windows Jako člen skupiny administrátorů na systémech Windows .

- Zadejte jeden z následujících příkazů:
  – Chcete-li zrušit nastavení primární instalace pomocí cesty k instalaci, kterou již nechcete mít jako primární instalaci, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -x -p MQ_INSTALLATION_PATH
```

– Chcete-li zrušit nastavení primární instalace pomocí názvu instalace, kterou již nechcete mít jako primární instalaci, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -x -n installationName
```

Související úlohy
Odinstalace, upgrade a údržba primární instalace
Výběr názvu instalace
Související odkazy
Funkce, které lze použít pouze s primární instalací na systému Windows
Externí knihovna a řídicí příkazové odkazy na primární instalaci na systému AIX and Linux
setmqinst

ALW Přidružení správce front k instalaci

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

Informace o této úloze

Instalace, ke které je správce front přidružen, omezuje tohoto správce front tak, aby mohl být spravován pouze příkazy z této instalace. Existují tři klíčové výjimky:

- **setmqm** změní instalaci přidruženou ke správci front. Tento příkaz musí být zadán z instalace, kterou chcete přidružit ke správci front, nikoli z instalace, ke které je správce front aktuálně přidružen. Název instalace určený příkazem **setmqm** se musí shodovat s instalací, ze které byl příkaz vydán.
- Produkt **strmqm** musí být vydán z instalace, která je přidružena ke správci front.

- V části **dspmq** jsou zobrazeny informace o všech správcích front v systému, nikoli pouze o správcích front přidružených ke stejné instalaci jako příkaz **dspmq** . Příkaz `dspmq -o installation` zobrazí informace o tom, kteří správci front jsou přidruženi k jakým instalacím.

V případě prostředí s vysokou dostupností příkaz **addmqinf** automaticky přidruží správce front k instalaci, ze které byl vydán příkaz **addmqinf** . Po dobu, kdy je příkaz **strmqm** vydán ze stejné instalace jako příkaz **addmqinf** , není nutné žádné další nastavení. Chcete-li spustit správce front pomocí jiné instalace, musíte nejprve změnit přidruženou instalaci pomocí příkazu **setmqm** .

Chcete-li přidružit správce front k instalaci, můžete použít příkaz **setmqm** následujícími způsoby:

- Přesouvání jednotlivých správců front mezi ekvivalentními verzemi produktu IBM MQ. Například přesunutí správce front z testu do produkčního systému.
- Migrace jednotlivých správců front ze starší verze produktu IBM MQ na novější verzi produktu IBM MQ. Migrace správců front mezi verzemi má různé důsledky, které musíte mít na paměti. Další informace o migraci viz Údržba a migrace.

Postup

1. Zastavte správce front pomocí příkazu **endmqm** z instalace, která je aktuálně přidružena ke správci 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 v části Installation2:

   ```
   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 potřebnou migraci správce front a způsobí, že správce front bude připraven k použití.

Jak pokračovat dále

Pokud byla odstraněna instalace, ke které je přidružen správce front, nebo pokud nejsou k dispozici informace o stavu správce front, příkaz **setmqm** nepřidruží správce front k jiné instalaci. V této situaci proveďte následující akce:

1. Pomocí příkazu **dspmqinst** můžete zobrazit další instalace v systému.
2. Ručně upravte pole `InstallationName` sekce `QueueManager` v souboru mqs.ini tak, aby uváděla jinou instalaci.
3. Pomocí příkazu **dltmqm** z této instalace odstraňte správce front.

Související pojmy

“Vyhledání instalací produktu IBM MQ v systému” na stránce 453
Máte-li v systému více instalací produktu IBM MQ , můžete zkontrolovat, které verze jsou nainstalovány a kde jsou.

“IBM MQ konfigurační soubor mqs.ini” na stránce 85
Konfigurační soubor IBM MQ `mqs.ini`obsahuje informace důležité pro všechny správce front v uzlu. Vytvoří se automaticky během instalace.

Související úlohy

Výběr primární instalace

Související odkazy

addmqinf

-živec

dspmqinst

endmqm
setmqm
strmqm

ALW Vyhledání instalací produktu IBM MQ v systému

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

K vyhledání instalací produktu IBM MQ v systému můžete použít následující metody:

- Pomocí instalačních nástrojů platformy se dotazujte, kde byl nainstalován produkt IBM MQ . Pak použijte příkaz **dspmqver** z instalace produktu IBM MQ . Následující příkazy jsou příklady příkazů, které můžete použít k dotazování, kde byl nainstalován produkt IBM MQ :
  - AIX Na systémech AIX můžete použít příkaz **lslpp** :

    ```
    lslpp -R ALL -l mqm.base.runtime
    ```

  - Linux Na systémech Linux můžete použít příkaz **rpm** :

    ```
    rpm -qa --qf "%{NAME}-%{VERSION}-%{RELEASE}\t%{INSTPREFIXES}\n" | grep MQSeriesRuntime
    ```

  - Windows Na systémech Windows můžete použít příkaz **wmic** . Tento příkaz může nainstalovat klienta wmic:

    ```
    wmic product where "(Name like '%MQ%') AND (not Name like '%bitSupport')" get Name,
    Version, InstallLocation
    ```

- Linux AIX V systémech AIX and Linux zadejte následující příkaz, abyste zjistili, kde byl nainstalován produkt IBM MQ :

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

  Pak použijte příkaz **dspmqver** z instalace produktu IBM MQ .

- Windows Chcete-li zobrazit podrobnosti o instalacích v systému, ve 32bitovém systému Windowszadejte následující příkaz:

  ```
  reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere MQ\Installation" /s
  ```

- Windows V 64bitovém systému Windowszadejte následující příkaz:

  ```
  reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IBM\WebSphere MQ\Installation" /s
  ```

Související odkazy
Příkaz dspmqver
dspmqinst
Více instalací

Konfigurace vysoké dostupnosti, zotavení a restartování

Aplikace lze nastavit jako vysoce dostupné udržováním dostupnosti fronty v případě selhání správce front a obnovením zpráv po selhání serveru nebo úložiště.

Informace o této úloze

z/OS V systému z/OSje vysoká dostupnost vestavěna do platformy. Viz Sdílené fronty a skupiny sdílení front.

Multi V systému Multiplatformsmůžete zlepšit dostupnost aplikací klienta pomocí opětovného připojení klienta k automatickému přepnutí klienta mezi skupinou správců front nebo k nové aktivní instanci správce front s více instancemi po selhání správce front. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů. Správce front s více instancemi je konfigurován tak, aby se spouštěl jako jeden správce front na více serverech. Do tohoto správce front implementujete serverové aplikace. Pokud server, na kterém je spuštěna aktivní instance, selže, provedení se automaticky přepne na záložní instanci stejného správce front na jiném serveru. Pokud nakonfigurujete serverové aplikace tak, aby byly spouštěny jako služby správce front, budou restartovány, jakmile se záložní instance stane aktivně spuštěnou instancí správce front.

Dalším způsobem, jak zvýšit dostupnost serverových aplikací na platformě Multiplatforms, je implementace serverových aplikací do více počítačů v klastru správců front. Od IBM WebSphere MQ 7.1 dále, operace zotavení z chyb klastru, které způsobily problémy, až do vyřešení problémů. Viz Změny v zotavení z chyb klastru na jiných serverech než z/OS. Produkt IBM MQ for Multiplatforms můžete také nakonfigurovat jako součást řešení klastrování specifického pro platformu, například:

- Microsoft Klastrovaný server
- IBM i Klastry HA na systému IBM i
- Linux AIX PowerHA pro AIX (dříve HACMP na AIX) a další řešení klastrování UNIX and Linux

Linux V systémech Linux můžete nakonfigurovat správce front replikovaných dat (RDQM) tak, aby implementoval řešení vysoké dostupnosti nebo zotavení z havárie. V případě vysoké dostupnosti jsou instance stejného správce front konfigurovány v každém uzlu ve skupině tří serverů Linux . Jedna ze tří instancí je aktivní instance. Data z aktivního správce front jsou synchronně replikována do dalších dvou instancí, takže jedna z těchto instancí může převzít v případě selhání. V případě zotavení z havárie je správce front spuštěn v primárním uzlu na jednom serveru, přičemž sekundární instance tohoto správce front je umístěna v uzlu zotavení na jiném serveru. Data jsou replikována mezi primární instancí a sekundární instancí, a pokud je primární uzel z nějakého důvodu ztracen, může být sekundární instance vytvořena do primární instance a spuštěna.

CP4I Nativní HA je řešení vysoké dostupnosti zaměřené na kontejnery. Nativní vysoká dostupnost používá replikaci protokolu k uchování tří instancí správce front spuštěných na různých uzlech v aktuálním stavu. Jedna instance je aktivní v libovolném okamžiku a zpracovává zprávy. Aktivní správce front odešle aktualizace protokolu ostatním dvěma instancím, aby je udržel aktualizované. Pokud aktivní instance selže, jedna z instancí repliky automaticky převezme aktivní roli.

MQ Appliance Další volbou pro řešení vysoké dostupnosti nebo zotavení z havárie je implementace dvojice zařízení IBM MQ . Viz Vysoká dostupnost a Zotavení z havárie v dokumentaci k produktu IBM MQ Appliance .

Systém zpráv zajišťuje, aby zprávy zadané do systému byly doručeny do místa určení. Produkt IBM MQ může trasovat trasu zprávy při jejím přesunu z jednoho správce front do jiného pomocí příkazu **dspmqrte** . Pokud dojde k selhání systému, lze zprávy obnovit různými způsoby v závislosti na typu selhání a způsobu, jakým je systém konfigurován. Produkt IBM MQ udržuje protokoly pro zotavení aktivit správců front, kteří zpracovávají příjem, přenos a doručování zpráv.Používá tyto protokoly pro tři typy zotavení:

1. *Obnova po restartu*, když zastavíte IBM MQ plánovaným způsobem.
2. *Obnova po selhání*, když se selhání zastaví IBM MQ.
3. *Obnova médií*pro obnovu poškozených objektů.

Ve všech případech obnova obnoví správce front do stavu, ve kterém se nacházel při zastavení správce front, s tou výjimkou, že všechny probíhající transakce jsou odvolány a z front budou odebrány všechny aktualizace, které probíhaly v době, kdy byl správce front zastaven. Obnova obnoví všechny trvalé zprávy; přechodné zprávy mohou být během procesu ztraceny.

POZOR: Protokoly pro zotavení nelze přesunout do jiného operačního systému.

Automatické opětovné připojení klienta

Klientské aplikace se mohou znovu připojit automaticky, aniž by bylo nutné psát další kód, a to konfigurací několika 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.

Naopak ruční opětovné připojení vyžaduje, aby aplikace klienta znovu vytvořila připojení pomocí `MQCONN` nebo `MQCONNX` a znovu otevřela objekty. Automatické opětovné připojení klienta je vhodné pro řadu aplikací klienta, nikoliv však pro všechny.

Tabulka 30 na stránce 456 uvádí nejstarší vydání podpory klienta IBM MQ , která musí být nainstalována na pracovní stanici klienta. Chcete-li pro aplikaci používat automatické opětovné připojení klienta, musíte provést upgrade pracovních stanic klienta na jednu z těchto úrovní. Tabulka 31 na stránce 456 uvádí další požadavky pro povolení automatického opětovného připojení klienta.

Při přístupu programu k volbám opětovného připojení může klientská aplikace nastavit volby opětovného připojení. S výjimkou klientů JMS a XMS , pokud má klientská aplikace přístup k volbám opětovného připojení, může také vytvořit obslužnou rutinu událostí pro zpracování událostí opětovného připojení.

Existující klientská aplikace může mít prospěch z podpory opětovného připojení bez opětovné kompilace a propojení:

- V případě klienta jiného nežJMS nastavte `mqclient.ini` proměnnou prostředí `DefRecon` tak, aby nastavovala volby opětovného připojení. Pomocí tabulky CCDT se připojte ke správci front. Pokud se má klient připojit ke správci front s více instancemi, zadejte v tabulce CCDT síťové adresy aktivních a rezervních instancí správce front. Pro správce front replikovaných dat nebo správce front HA na zařízení IBM MQ můžete zadat plovoucí adresu IP, kterou používají aktivní i rezervní správci front ke zjednodušení konfigurace.
- Pro klienta JMS nastavte volby opětovného připojení v konfiguraci továrny připojení. Při spuštění uvnitř kontejneru EJB serveru Java EE se mohou objekty MDB znovu připojit k produktu IBM MQ pomocí mechanizmu opětovného připojení poskytovaného specifikacemi aktivace adaptéru prostředků IBM MQ (nebo porty modulu listener, pokud jsou spuštěny v produktu WebSphere Application Server). Pokud však aplikace není MDB (nebo je spuštěna ve webovém kontejneru), musí implementovat vlastní logiku opětovného připojení, protože automatické opětovné připojení klienta není v tomto scénáři podporováno. Adaptér prostředků IBM MQ poskytuje tuto schopnost opětovného připojení pro doručení zpráv do objektů typu message-driven bean, ale ostatní prvky Java EE , jako například servlety, musí implementovat své vlastní opětovné připojení.

Poznámka: Automatické opětovné připojení klienta není podporováno produktem IBM MQ classes for Java.

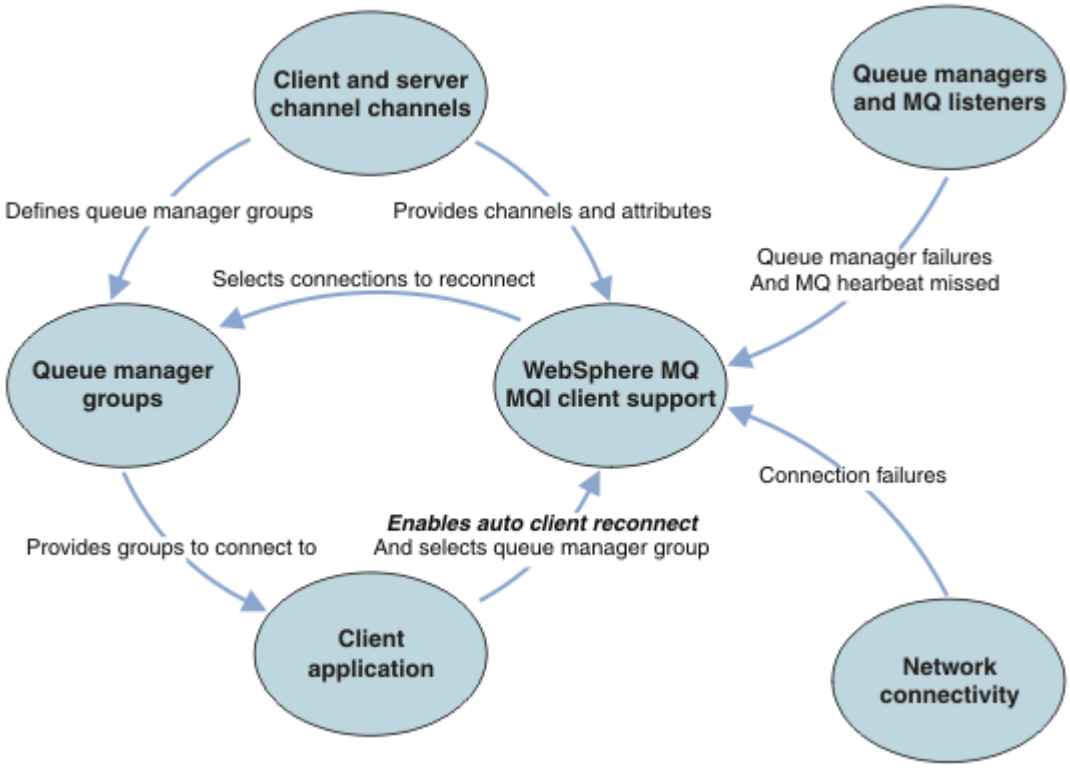
Tabulka 30. Podporovaní klienti			
Rozhraní klienta	**Klient**	**Přístup programu k volbám opětovného připojení**	**Podpora opětovného připojení**
Rozhraní API systému zpráv	C, C + +, COBOL, Nespravovaný jazyk Visual Basic, XMS (Nespravovaný XMS na systému Windows)	7.0.1	7.0.1
	JMS (kontejner klienta JSE a Java EE a spravované kontejnery)	7.0.1.3	7.0.1.3
	IBM MQ classes for Java	Nepodporováno	Nepodporováno
	Spravovaní klienti XMS a spravovaní klienti .NET : C#, Visual Basic,	7.1	7.1
Další rozhraní API	Windows Communication Foundation (nespravováno [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. Nastavte spravovaný nebo nespravovaný režim v konfiguraci vazby WCF.

Automatické opětovné připojení má následující konfigurační požadavky:

Tabulka 31. Požadavky na automatickou konfiguraci opětovného připojení		
Komponenta	**Požadavek**	**Účinek nesplnění požadavku**
instalace produktu IBM MQ MQI client	Viz téma Tabulka 30 na stránce 456	`MQRC_OPTIONS_ERROR`
IBM MQ Instalace serveru	Úroveň 7.0.1	`MQRC_OPTIONS_ERROR`
Kanál	`SHARECNV > 0`	`MQRC_ENVIRONMENT_ERROR`
prostředí aplikace	Musí být ve vláknech	`MQRC_ENVIRONMENT_ERROR`
MQI	Jedna z těchto možností: • `MQCONNX` s volbou `MQCNO` `Volby` nastavenou na `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR`. • `Defrecon=YES|QMGR` je v `mqclient.ini` • V souboru JMS nastavte vlastnost **`CLIENTRECONNECTOPTIONS`** továrny připojení.	`MQCC_FAILED` v případě přerušení připojení nebo ukončení či selhání správce front.

Obrázek 68 na stránce 457 zobrazuje hlavní interakce mezi komponentami, které jsou zapojeny do opětovného připojení klienta.



Obrázek 68. Automatické opětovné připojení klienta

Aplikace klienta

Klientská aplikace je IBM MQ MQI client. Podrobnosti o automatickém opětovném připojení klienta pro klienta JMS naleznete v tématu Použití automatického JMS opětovného připojení klienta.

- Standardně nejsou klienti automaticky znovu připojeni. Povolte automatické opětovné připojení klienta nastavením volby `MQCONNX` `MQCNO` `Volba` `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR`.
- Mnoho aplikací je napsáno tak, aby byly schopny využít automatického opětovného připojení bez dalšího kódování. Povolte automatické opětovné připojení pro existující programy bez provedení změn kódu nastavením atributu `DefRecon` v sekci kanálů konfiguračního souboru `mqclient.ini` .
- Použijte jednu z těchto tří voleb:

  1. Upravte program tak, aby logika znovu neovlivňovala připojení. Můžete například zadat volání `MQI` v rámci synchronizačního bodu a znovu odeslat zálohované transakce. Asynchronní spotřebitelé by měli zkontrolovat, zda byli 'pozastaveni', pokud je transakce odvolána.
  2. Přidejte obslužnou rutinu událostí pro zjištění opětovného připojení a obnovení stavu klientské aplikace při opětovném navázání připojení.
  3. Nepovolujte automatické opětovné připojení: místo toho odpojte klienta a zadejte nové volání `MQCONN` nebo `MQCONNX` `MQI`, abyste nalezli jinou instanci správce front, která je spuštěna ve stejné skupině správců front.

  Další podrobnosti o těchto třech volbách viz “Obnova aplikace” na stránce 543.
- Opětovné připojení ke správci front se stejným názvem nezaručuje, že jste se znovu připojili ke stejné instanci správce front.

Chcete-li se znovu připojit k instanci stejného správce front, použijte volbu MQCNO MQCNO_RECONNECT_Q_MGR.

- Klient může registrovat obslužnou rutinu událostí, aby mohl být informován o stavu opětovného připojení. Položku MQHCONN předanou v obslužné rutině událostí nelze použít. K dispozici jsou následující kódy příčiny:

  MQRC_RECONNECTING
  Připojení se nezdařilo a systém se pokouší o opětovné připojení. Pokud se provede více pokusů o opětovné připojení, obdržíte více událostí MQRC_RECONNECTING .

  MQRC_RECONNECTED
  Bylo provedeno opětovné připojení a všechny manipulátory byly úspěšně znovu zavedeny.

  MQRC_RECONNECT_FAILED
  Opětovné připojení nebylo úspěšné.

  MQRC_RECONNECT_QMID_MISMATCH
  Bylo zadáno znovu připojitelné připojení MQCNO_RECONNECT_Q_MGR a připojení se pokusilo znovu připojit k jinému správci front.

  MQRC_RECONNECT_Q_MGR_REQD
  Volba, jako např. MQMO_MATCH_MSG_TOKEN ve volání MQGET , byla uvedena v klientském programu, který vyžaduje opětovné připojení ke stejnému správci front.

- Znovu připojitelný klient je schopen se automaticky znovu připojit pouze po připojení. To znamená, že samotné volání MQCONNX se znovu nezkusí, pokud selže. Pokud například obdržíte návratový kód 2543 - MQRC_STANDBY_Q_MGR z MQCONNX, znovu vyvolejte volání po krátké prodlevě.

  MQRC_RECONNECT_INCOMPATIBLE
  Tento kód příčiny je vrácen, když se aplikace pokusí použít MQPMO_LOGICAL_ORDER (s MQPUT a MQPUT1) nebo MQGMO_LOGICAL_ORDER (s MQGET) když jsou nastaveny volby opětovného připojení. Důvodem pro vrácení kódu příčiny je zajistit, aby aplikace v takových případech nikdy nepoužívaly opětovné připojení.

  MQRC_CALL_PŘERUŠENO
  Tento kód příčiny je vrácen, když dojde k přerušení připojení během provádění volání Commit a klient se znovu připojí. Výsledkem operace MQPUT trvalé zprávy mimo synchronizační bod je také vrácení stejného kódu příčiny do aplikace.

Správci front s vysokou dostupností

Správci front s vysokou dostupností mají aktivní instanci a jednu nebo více instancí správce front v pohotovostním režimu. Aktivní správce front je synchronizován se správci front v pohotovostním režimu, takže v případě selhání aktivní instance jej může rezervní databáze automaticky převzít. Existuje řada různých řešení, která poskytují správce front s vysokou dostupností. Viz “Konfigurace vysoké dostupnosti” na stránce 465.

Můžete zjednodušit restartování aplikací IBM MQ MQI client poté, co správce front s vysokou dostupností aktivoval svou instanci v pohotovostním režimu, pomocí automatického opětovného připojení klienta.

Pohotovostní instance správce front s vysokou dostupností se obvykle nachází na jiné síťové adrese než aktivní instance. Do tabulky CCDT (Client Connection Definition Table) zahrňte síťové adresy obou instancí. Buď zadejte seznam síťových adres pro parametr **CONNAME** , nebo definujte více řádků pro správce front v tabulce CCDT. Správci front replikovaných dat a správci front s vysokou dostupností zařízení IBM MQ podporují plovoucí adresy IP, kde můžete zadat jedinou adresu pro použití s aktivními nebo rezervními správci front.

Skupiny správců front

Obvykle se produkt IBM MQ MQI clients znovu připojí k libovolnému správci front ve skupině správců front. Někdy chcete, aby se agent IBM MQ MQI client znovu připojil pouze ke stejnému správci front. Může mít afinitu ke správci front.

Můžete určit, zda se aplikace klienta vždy připojí a znovu připojí ke správci front se stejným názvem, ke stejnému správci front nebo k libovolné sadě správců front, které jsou definovány se stejnou hodnotou QMNAME v tabulce připojení klienta.

- Atribut názvu správce front QMNAMEv definici kanálu klienta je názvem skupiny správců front.
- Pokud v klientské aplikaci nastavíte hodnotu parametru MQCONN nebo MQCONNX QmgrName na název správce front, klient se připojí pouze ke správcům front s tímto názvem. Pokud před název správce front vložíte hvězdičku (*), klient se připojí k libovolnému správci front ve skupině správců front se stejnou hodnotou QMNAME . Úplné vysvětlení naleznete v tématu Skupiny správců front v tabulce CCDT.

Klientovi můžete zabránit v opětovném připojení k jinému správci front. Nastavte volbu MQCNO , MQCNO_RECONNECT_Q_MGR. Příkaz IBM MQ MQI client se nezdaří, pokud se znovu připojí k jinému správci front. Pokud nastavíte volbu MQCNO MQCNO_RECONNECT_Q_MGR, nezahrnujte do stejné skupiny správců front další správce front. Klient vrátí chybu, pokud správce front, ke kterému se znovu připojí, není stejný správce front jako ten, ke kterému se připojil.

Skupiny sdílení front

z/OS Automatické opětovné připojení klienta ke skupinám sdílení front z/OS používá stejné mechanizmy pro opětovné připojení jako jakékoli jiné prostředí. Klient se znovu připojí ke stejnému výběru správců front, který je konfigurován pro původní připojení. Pokud například používáte tabulku definic kanálů klienta, administrátor by měl zajistit, že všechny položky v tabulce budou interpretovat stejnou skupinu sdílení front z/OS .

Definice kanálů klienta a serveru

Definice kanálů klienta a serveru definují skupiny správců front, ke kterým se může aplikace klienta znovu připojit. Definice řídí výběr a časování opětovných připojení a další faktory, jako například zabezpečení; viz související témata. Nejdůležitější atributy kanálu, které je třeba zvážit pro opětovné připojení, jsou uvedeny 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.

z/OS Všimněte si, že KAINT platí pouze pro z/OS .

Název správce front (QMNAME) QMNAME
Název správce front.

Atributy připojení serveru

Interval prezenčního signálu (HBINT) HBINT
Interval prezenčního signálu. Nastavte interval synchronizace na kanálu připojení klienta.

Interval udržení aktivity (KAINT) KAINT
Interval udržení aktivity. Nastavte interval udržení aktivity na kanálu připojení klienta.

z/OS Všimněte si, že KAINT platí pouze pro z/OS .

KAINT je prezenční signál síťové vrstvy a HBINT je prezenční signál IBM MQ mezi klientem a správcem front. Nastavení těchto prezenčních signálů na kratší dobu slouží ke dvěma účelům:

1. Díky simulaci aktivity na připojení je méně pravděpodobné, že software síťové vrstvy, který je zodpovědný za zavírání neaktivních připojení, ukončí vaše připojení.
2. Je-li připojení ukončeno, dojde ke zkrácení prodlevy před zjištěním přerušeného připojení.

Výchozí interval udržení aktivity TCP/IP jsou 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 pouhých 10 minutách.

Síťová konektivita

Pouze selhání sítě, která jsou předána do produktu IBM MQ MQI client sítí, jsou zpracována funkcí automatického opětovného připojení klienta.

- Opětovná připojení prováděná automaticky přenosem jsou pro produkt IBM MQneviditelná.
- Nastavení HBINT pomáhá vypořádat se se selháním sítě, která jsou pro produkt IBM MQneviditelná.

Správci front a moduly listener IBM MQ

Opětovné připojení klienta je spuštěno selháním serveru, selháním správce front, selháním síťové konektivity a přepnutím administrátora na jinou instanci správce front.

- Používáte-li správce front s více instancemi, dojde při přepínání řízení z aktivní instance správce front na instanci v pohotovostním režimu k další příčině opětovného připojení klienta.
- Ukončení správce front pomocí výchozího příkazu **endmqm** nespustí automatické opětovné připojení klienta. Přidejte volbu `-r` do příkazu **endmqm** , chcete-li požadovat automatické opětovné připojení klienta, nebo volbu `-s` , chcete-li po vypnutí přenést do instance správce front v pohotovostním režimu.

Podpora automatického opětovného připojení IBM MQ MQI client

Pokud v produktu IBM MQ MQI clientpoužíváte podporu automatického opětovného připojení klienta, aplikace klienta se automaticky znovu připojí a bude pokračovat ve zpracování, aniž byste vyvolali volání MQCONN nebo MQCONNX MQI pro opětovné připojení ke správci front.

- Automatické opětovné připojení klienta je spuštěno jedním z následujících výskytů:
  - Selhání správce front
  - Ukončení správce front a zadání volby `-r`, reconnect, v příkazu **endmqm**
- Volby produktu MQCONNX MQCNO řídí, zda jste povolili automatické opětovné připojení klienta. Volby jsou popsány v části Volby opětovného připojení.
- Automatické opětné připojení klienta vyvolá volání MQI jménem vaší aplikace za účelem obnovení manipulátoru připojení a manipulátorů pro jiné otevřené objekty, aby mohl váš program pokračovat v běžném zpracování poté, co zpracoval jakékoli chyby MQI, které vyplynuly z přerušeného připojení. Viz “Obnova automaticky znovu připojeného klienta” na stránce 545.
- Pokud jste pro připojení napsali program uživatelské procedury kanálu, tato uživatelská procedura obdrží tato další volání MQI.
- Můžete registrovat obslužnou rutinu událostí opětovného připojení, která se spustí při zahájení opětovného připojení a po jeho dokončení.

Ačkoli zamýšlená doba opětovného připojení není delší než jedna minuta, opětovné připojení může trvat déle, protože správce front může mít mnoho prostředků ke správě. Během této doby může aplikace klienta zadržovat zámky, které nepatří k prostředkům IBM MQ . Existuje hodnota časového limitu, kterou můžete nakonfigurovat tak, aby omezila dobu, po kterou klient čeká na opětovné připojení. Hodnota (v sekundách) je nastavena v souboru `mqclient.ini` .

```
Channels:
MQReconnectTimeout = 1800
```

Po vypršení časového limitu se neprovedou žádné pokusy o opětovné připojení. Když systém zjistí, že vypršel časový limit, vrátí chybu MQRC_RECONNECT_FAILED .

Související pojmy

Opakovaně připojitelní klienti

Související úlohy

Zastavení správce front

z/OS Monitorování zpráv konzoly

V systému IBM MQ for z/OSexistuje řada informačních zpráv vydaných správcem front nebo inicializátorem kanálu, které by měly být považovány za zvlášť významné. Tyto zprávy samy o sobě neindikují problém, ale mohou být užitečné při sledování, protože indikují potenciální problém, který může vyžadovat adresování.

Přítomnost těchto zpráv konzoly může také znamenat, že uživatelská aplikace vkládá do sady stránek velký počet zpráv, což může být příznakem většího problému:

- Problém s uživatelskou aplikací, která zprávy PUTs, jako například nekontrolovaná smyčka.
- Uživatelská aplikace, která získává zprávy z fronty, již nefunguje.

Zprávy konzoly k monitorování

Následující seznam nastiňuje zprávy, které mohou potenciálně označovat větší problémy. Určete, zda je nutné sledovat tyto zprávy pomocí automatizace systému a poskytněte odpovídající dokumentaci, aby bylo možné efektivně sledovat případné problémy.

CSQI004I: *název-csect* ZVÁŽIT INDEXOVÁNÍ *název-fronty* BY *typ-indexu* FOR *typ-připojení* CONNECTION *název-připojení*, *počet-zpráv* PŘESKOČENÉ ZPRÁVY

- Správce front zjistil, že aplikace přijímá zprávy podle ID zprávy nebo ID korelace z fronty, pro kterou není definován index.
- Zvažte vytvoření indexu pro identifikovanou frontu změnou lokálního objektu fronty *název_fronty*, atributu INDXTYPE na hodnotu *typ_indexu*.

CSQI031I: *csect-name* NOVÁ OBLAST PRO ROZŠÍŘENÍ SADY STRÁNEK *psid* ÚSPĚŠNĚ NAFORMÁTOVÁNO

- Zkontrolujte hloubku front přidělených této sadě stránek.
- Zjistěte příčinu selhání při zpracování zpráv.

.

CSQI041I: *název_csect* JOB *název_úlohy* USER *ID_uživatele* DOŠLO K CHYBĚ PŘI PŘÍSTUPU K SADĚ STRÁNEK *psid*

- Určete, zda je sada stránek přidělena správci front.
- Zadáním příkazu **DISPLAY USAGE** určete stav sady stránek.
- Další chybové zprávy naleznete v protokolu úlohy správce front.

.

CSQI045I: *csect-name* Protokol RBA dosáhl hodnoty *rba*. Naplánovat reset protokolu

- Naplánujte zastavení správce front ve vhodnou dobu a resetujte protokoly.
- Pokud váš správce front používá 6bajtové protokoly RBA protokolu, zvažte převod správce front na 8bajtové protokoly RBAs protokolu.

CSQI046E: *csect-name* Protokol RBA dosáhl hodnoty *rba*. Provést reset protokolu

- Naplánujte zastavení správce front ve vhodnou dobu a resetujte protokoly.
- Pokud váš správce front používá 6bajtové protokoly RBA protokolu, zvažte převod správce front na 8bajtové protokoly RBAs protokolu.

CSQI047E: *csect-name* Protokol RBA dosáhl hodnoty *rba*. Zastavit správce front a resetovat protokoly

- Okamžitě zastavte správce front a resetujte protokoly.
- Pokud váš správce front používá 6bajtové protokoly RBA protokolu, zvažte převod správce front na 8bajtové protokoly RBAs protokolu.

CSQJ004I: ACTIVE LOG COPY *n* INACTIVE, LOG IN SINGLE MODE, ENDRBA= *ttt*

- Správce front aktivoval režim transakčního protokolování 'single'. To často svědčí o problému s odlehčením protokolu.
- Zadáním příkazu **DISPLAY LOG** určete nastavení pro oboustranný tisk aktivních a archivních protokolů. Tato obrazovka také zobrazuje, kolik aktivních protokolů vyžaduje zpracování odlehčování.
- Další chybové zprávy naleznete v protokolu úlohy správce front.

CSQJ031D: *csect-name*, ROZSAH PROTOKOLU RBA MUSÍ BÝT RESETOVÁN. ODPOVĚZTE 'Y', CHCETE-LI POKRAČOVAT VE SPUŠTĚNÍ, NEBO ' N', CHCETE-LI UKONČIT PRÁCI

- Zastavte správce front a resetujte protokoly co nejdříve a resetujte protokoly.
- Pokud váš správce front používá 6bajtové protokoly RBA protokolu, zvažte převod správce front na 8bajtové protokoly RBAs protokolu.

CSQJ032E: *csect-name alert-lvl* -BLÍŽÍCÍ SE KONEC ROZSAHU RBA PROTOKOLU *max-rba*. CURRENT LOG RBA IS *current-rba*.

- Naplánujte zastavení správce front a co nejdříve resetujte protokoly.
- Pokud váš správce front používá 6bajtové protokoly RBA protokolu, zvažte převod správce front na 8bajtové protokoly RBAs protokolu.

CSQJ110E: POSLEDNÍ KOPIE*n* AKTIVNÍ DATOVÉ SADY PROTOKOLU *nnn* PROCENTO PLNÉ

- Proveďte kroky k dokončení dalších čekajících úloh odlehčování provedením požadavku na zobrazení, abyste určili nevyřízené požadavky související s procesem odlehčování protokolu. Proveďte potřebné akce, abyste splnili všechny požadavky, a povolte odlehčování, abyste mohli pokračovat.
- Zvažte, zda existuje dostatek datových sad aktivního protokolu. V případě potřeby můžete dynamicky přidávat další datové sady protokolu pomocí příkazu DEFINE LOG .

CSQJ111A: NEDOSTATEK PROSTORU V DATOVÝCH SADÁCH AKTIVNÍHO PROTOKOLU

- Proveďte požadavek na zobrazení, abyste se ujistili, že neexistují žádné neprovedené požadavky související s procesem odlehčování protokolu. Proveďte potřebné akce, abyste splnili všechny požadavky, a povolte odlehčování, abyste mohli pokračovat.
- Zvažte, zda existuje dostatek datových sad aktivního protokolu. V případě potřeby můžete dynamicky přidávat další datové sady protokolu pomocí příkazu DEFINE LOG .
- Pokud byla prodleva způsobena nedostatkem prostředku vyžadovaného pro odlehčování, musí být k dispozici nezbytný prostředek, aby bylo možné odlehčování dokončit, a tak pokračovat v protokolování. Informace o zotavení z této podmínky naleznete v tématu Problémy protokolu archivace.

CSQJ114I: CHYBA NA DATOVOU SADU ARCHIVU, ODLEHČOVÁNÍ POKRAČUJE S GENEROVÁNÍM POUZE JEDNÉ DATOVÉ SADY ARCHIVU

- Další chybové zprávy naleznete v protokolu úlohy správce front.
- Vytvořte druhou kopii protokolu archivu a aktualizujte BSDS ručně.

CSQJ115E: OPERACE OFFLOAD SELHALA, NELZE PŘIDĚLIT DATOVOU SADU ARCHIVU

Přezkoumejte informace o chybovém stavu zprávy CSQJ103E nebo CSQJ073E. Opravte stav, který způsobil chybu alokace datové sady, aby při opakovaném pokusu mohlo dojít k odlehčování.

CSQJ136I: NELZE PŘIDĚLIT PÁSKOVOU JEDNOTKU PRO PŘIPOJENÍ-ID= *xxxx* KORELACE-ID= *rrrrrr*, *m* PŘIDĚLENO *n* POVOLENO

- Další chybové zprávy naleznete v protokolu úlohy správce front.

.

CSQJ151I: *csect-name* ERROR READING RBA *rrr*, CONNECTION-ID= *xxxx* CORRELATION-ID= *rrrrrr* PŘÍČINA CODE= *ccc*

- Další zprávy naleznete v protokolu úlohy správce front.
- Zadáním příkazu **DISPLAY CONN** určete, které připojení nepotvrzuje svou aktivitu.
- Ujistěte se, že aplikace může potvrdit své aktualizace.

CSQJ160I: BYLO NALEZENO PŘERUŠITELNÉ UOW, URID= *urid* CONNECTION NAME= *name*

- Další zprávy naleznete v protokolu úlohy správce front.
- Zadáním příkazu **DISPLAY CONN** určete, které připojení nepotvrzuje svou aktivitu.
- Ujistěte se, že aplikace může potvrdit své aktualizace.

CSQJ161I: TRANSAKCE NEVYŘEŠENÉ PO *n* OFFLOADS, URID= *urid* CONNECTION NAME= *name*

- Určete, zda je sada stránek přidělena správci front.
- Zadáním příkazu **DISPLAY USAGE** určete stav sady stránek.
- Další zprávy naleznete v protokolu úlohy správce front.

CSQP011E: STAV CHYBY PŘIPOJENÍ *ret-code* FOR PAGE SET *psid*

- Zkontrolujte hloubku front přidělených této sadě stránek.
- Zjistěte příčinu selhání při zpracování zpráv.

CSQP013I: *csect-name* NOVÁ OBLAST VYTVOŘENÁ PRO SADU STRÁNEK psid. NOVÝ ROZSAH BUDE NYNÍ FORMÁTOVÁN

- Zkontrolujte hloubku front přidělených této sadě stránek.
- Zjistěte příčinu selhání při zpracování zpráv.
- Určete, zda je třeba fronty přemístit do jiné sady stránek.
- Pokud je svazek plný, určete, zda potřebujete nastavit sadu stránek jako datovou sadu s více svazky. Pokud je sada stránek již více svazků, zvažte přidání dalších svazků do používané skupiny úložišť. Jakmile je k dispozici více místa, zopakujte expanzi nastavením metody **EXPAND** pro nastavení stránky na hodnotu **SYSTEM**. Je-li vyžadováno opakování, přepněte volbu **EXPAND** na hodnotu **SYSTEM** a poté se vraťte k normálnímu nastavení.

CSQP014E: *csect-name* ROZŠÍŘENÍ SELHALO PRO SADU STRÁNEK psid. BUDOUCÍ POŽADAVKY NA ROZŠÍŘENÍ BUDOU ODMÍTNUTY

- Zkontrolujte hloubku front přidělených této sadě stránek.
- Zjistěte příčinu selhání při zpracování zpráv.
- Určete, zda je třeba fronty přemístit do jiné sady stránek.

CSQP016E: *csect-name* PAGE SET *psid* DOSÁHL MAXIMÁLNÍHO POČTU OBLASTÍ PRO ROZŠÍŘENÍ. NELZE JI ZNOVU ROZŠÍŘIT

- Zkontrolujte hloubku front přidělených této sadě stránek.
- Zjistěte příčinu selhání při zpracování zpráv.

CSQP017I: *csect-name* ROZŠÍŘENÍ SPUŠTĚNO PRO SADU STRÁNEK *psid*

Zadejte příkazy DISPLAY THREAD, abyste určili stav jednotek práce v produktu IBM MQ.

CSQP047E: Nedostupné sady stránek mohou způsobit problémy-proveďte akci k nápravě této situace

- Postupujte podle odezvy systémového programátora.

CSQQ008I: *nn* jednotky zotavení jsou stále v nejistém stavu ve správci front *qqqq*

- Zjistěte stav fronty nedoručených zpráv. Ujistěte se, že fronta nedoručených zpráv není PUT zakázaná.
- Ujistěte se, že fronta nedoručených zpráv není na limitu MAXMSG.

CSQQ113I: *název_psb id-oblasti* Tuto zprávu nelze zpracovat

- Zkontrolujte datovou sadu CSQOUTX, abyste určili příčinu selhání CSQINPX.
- Některé příkazy nemusí být zpracovány.

CSQX035I: *csect-name* Připojení ke správci front *qmgr-name* zastaveno nebo přerušeno, MQCC= *mqcc* MQRC= *mqrc* (*mqrc-text*

- Zkontrolujte MQRC a určete příčinu selhání.
- Tyto kódy jsou dokumentovány ve zprávách produktu IBM MQ for z/OS , v kódu dokončení a v kódu příčiny.

CSQX032I: *název_csect* Obslužná rutina inicializačního příkazu byla ukončena

- Zkontrolujte MQRC a určete příčinu selhání.
- Tyto kódy jsou dokumentovány ve zprávách produktu IBM MQ for z/OS , v kódu dokončení a v kódu příčiny.

CSQX048I: *csect-name* Nelze převést zprávu pro *name*, MQCC= *mqcc* MQRC= *mqrc* (*mqrc-text*)

- Zkontrolujte protokol úlohy, abyste určili příčinu selhání TCP/IP.
- Zkontrolujte, zda adresní prostor TCP/IP neobsahuje chyby.

CSQX234I: *název_csect* Modul listener byl zastaven, TRPTYPE= *trptype* INDISP= *dispozice*

- Pokud se modul listener nezastaví, po provedení příkazu **STOP** zkontrolujte adresní prostor TCP/IP, zda neobsahuje chyby.
- Postupujte podle odezvy systémového programátora.

CSQX407I: *csect-name* Fronta klastru *q-name* nekonzistentní definice

- Více front klastru v rámci klastru má nekonzistentní hodnoty. Prošetřete a vyřešte rozdíly.

CSQX411I: *csect-name* Zastavený správce úložiště

- Pokud byl správce úložiště zastaven kvůli chybě, zkontrolujte zprávy v protokolu úlohy.

CSQX417I: *název_sekce_csect* Odejde odesilatelé klastru pro odebraného správce front *název_správce front*

- Postupujte podle odezvy systémového programátora.

CSQX418I: *csect-name* Pouze jedno úložiště pro klastr *cluster_name*

- Chcete-li zvýšit vysokou dostupnost, měly by být klastry nakonfigurovány se dvěma úplnými úložišti.

CSQX419I: *csect-name* Žádné přijímače klastru pro klastr *cluster_name*

- Postupujte podle odezvy systémového programátora.

CSQX420I: *csect-name* Žádná úložiště pro klastr *název_klastru*

- Postupujte podle odezvy systémového programátora.

CSQX448E: *csect-name* Správce úložiště se zastavuje kvůli chybám. Restart za *n* sekund

- Postupujte podle odezvy systémového programátora.

  Tato zpráva je vložena každých 600 sekund (10 minut) do SYSTEM.CLUSTER.COMMAND.QUEUE je povoleno pomocí příkazu:

```
ALTER QLOCAL(SYSTEM.CLUSTER.COMMAND.QUEUE) GET(ENABLED)
```

Před povolením fronty může být vyžadován ruční zásah pro vyřešení problému, který způsobil ukončení správce úložiště, před vydáním první zprávy CSQX448E .

CSQX548E: *csect-name* Zprávy odeslané do lokální fronty nedoručených zpráv, kanál *název_kanálu* reason=*mqrc* (*mqrc-text*)

- Postupujte podle odezvy systémového programátora.

CSQX788I: *csect-name* Vyhledávání DNS pro adresu *address* pomocí funkce '*func*' trvalo *n* sekund

- Postupujte podle odezvy systémového programátora.

CSQY225E: *název-csect* Správce front je kriticky krátký na lokální úložiště nad pruhem-provést akci

- Správce front má kriticky nedostatek virtuálního úložiště nad pruhem. Je třeba provést akci, která situaci zmírní, a vyhnout se možnému nestandardnímu ukončení správce front.

CSQ5038I: *název-csect* Úloha-služby-úlohy-nereaguje od hh.mm.ss.nnnnnn. Zkontrolujte problémy s produktem Db2

- Postupujte podle odezvy systémového programátora.

Konfigurace vysoké dostupnosti

Chcete-li pracovat se správci front IBM MQ v konfiguraci vysoké dostupnosti (HA), můžete nastavit správce front tak, aby pracoval se správcem vysoké dostupnosti, například PowerHA pro AIX (dříve HACMP). nebo pomocí služby MSCS (Microsoft Cluster Service) nebo pomocí správců front s více instancemi systému IBM MQ . V systémech Linux můžete také implementovat správce front replikovaných dat (RDQMs), kteří k zajištění vysoké dostupnosti používají skupinu založenou na kvótě. Další volba, Nativní HA, je zaměřena na nasazení kontejnerů.

MQ Appliance Další volbou pro řešení vysoké dostupnosti nebo zotavení z havárie je implementace dvojice zařízení IBM MQ . Viz Vysoká dostupnost a Zotavení z havárie v dokumentaci k produktu IBM MQ Appliance .

Musíte mít na paměti následující definice konfigurace:

Klastry správců front
Skupiny dvou nebo více správců front v jednom nebo více počítačích, které poskytují automatické propojení a umožňují sdílení front mezi nimi za účelem vyrovnání zátěže a redundance. Od IBM WebSphere MQ 7.1 dále, operace zotavení z chyb klastru, které způsobily problémy, až do vyřešení problémů.

Klastry HA
Klastry s vysokou dostupností jsou skupiny dvou nebo více počítačů a prostředků, jako jsou disky a sítě, vzájemně propojené a nakonfigurované tak, aby v případě selhání správce vysoké dostupnosti, například HACMP (AIX and Linux) nebo MSCS (Windows), provedl *překonání selhání*. Překonání selhání přenese data o stavu aplikací z počítače, který selhal, do jiného počítače v klastru a znovu zahájí jejich činnost v tomto klastru. To poskytuje vysokou dostupnost služeb spuštěných v klastru HA. Vztah mezi klastry IBM MQ a klastry HA je popsán v části “Vztah klastrů HA ke klastrům správců front” na stránce 467.

Správci front s více instancemi
Instance stejného správce front nakonfigurované na dvou nebo více počítačích. Spuštěním více instancí se jedna instance stane aktivní instancí a ostatní instance se stanou rezervními. Pokud aktivní instance selže, rezervní instance spuštěná na jiném počítači se automaticky převezme. Pomocí správců front s více instancemi můžete konfigurovat vlastní systémy zpráv s vysokou dostupností založené na produktu IBM MQ, aniž byste museli používat technologii klastrů, například HACMP nebo MSCS. Klastry HA a správci front s více instancemi jsou alternativními způsoby, jak učinit správce front vysoce dostupnými. Nekombinujte je vložením správce front s více instancemi do klastru HA.

Správci front replikovaných dat s vysokou dostupností (HA RDQMs)
Instance stejného správce front nakonfigurované na každém uzlu ve skupině tří serverů Linux . Jedna ze tří instancí je aktivní instance. Data z aktivního správce front jsou synchronně replikována do

dalších dvou instancí, takže jedna z těchto instancí může převzít v případě selhání. Seskupení serverů je řízeno pomocí Pacemakera replikace pomocí DRBD.

Správci front replikovaných dat zotavení z havárie (DR RDQMs)
Správce front je spuštěn v primárním uzlu na jednom serveru, přičemž sekundární instance tohoto správce front je umístěna v uzlu zotavení na jiném serveru. Data jsou replikována mezi primární instancí a sekundární instancí, a pokud je primární uzel z nějakého důvodu ztracen, může být sekundární instance vytvořena do primární instance a spuštěna. Oba uzly musí být servery Linux . Replikace je řízena DRBD.

Zotavení z havárie/správci front replikovaných dat s vysokou dostupností (DR/HA RDQM)
Můžete konfigurovat správce front replikovaných dat (RDQM), který je spuštěn ve skupině s vysokou dostupností na jednom serveru, ale může selhat v jiné skupině s vysokou dostupností na jiném serveru, pokud dojde k nějaké havárii, která způsobí nedostupnost první skupiny. Toto je známé jako DR/HA RDQM.

CP4I **Nativní vysoká dostupnost**
Nativní HA je řešení vysoké dostupnosti zaměřené na nasazení kontejnerů produktu IBM MQ. Nativní vysoká dostupnost používá replikaci protokolu k uchování tří instancí správce front spuštěných na různých uzlech v aktuálním stavu. Jedna instance je aktivní v libovolném okamžiku a zpracovává zprávy. Aktivní správce front odešle aktualizace protokolu ostatním dvěma instancím, aby je udržel aktualizované. Pokud aktivní instance selže, jedna z instancí repliky automaticky převezme aktivní roli.

Rozdíly mezi správci front s více instancemi a klastry HA

Správci front s více instancemi a klastry s vysokou dostupností jsou alternativními způsoby, jak dosáhnout vysoké dostupnosti pro vaše správce front. Zde jsou některé body, které zdůrazňují rozdíly mezi těmito dvěma přístupy.

Správci front s více instancemi zahrnují následující funkce:

- Základní podpora překonání selhání integrovaná do produktu IBM MQ
- Rychlejší překonání selhání než klastr s vysokou dostupností
- Jednoduchá konfigurace a ovládání
- Integrace s produktem IBM MQ Explorer

Omezení správců front s více instancemi zahrnují:

- Vyžaduje vysoce dostupné, vysoce výkonné síťové úložiště
- Složitější konfigurace sítě, protože správce front mění adresu IP v případě, že dojde k selhání

Klastry HA zahrnují následující funkce:

- Schopnost koordinovat více prostředků, například aplikační server nebo databáze.
- Flexibilnější volby konfigurace včetně klastrů obsahujících více než dva uzly
- Může provést překonání selhání vícekrát bez zásahu operátora
- Převzetí adresy IP správce front v rámci překonání selhání

Omezení klastrů HA zahrnují:

- Další nákup produktů a dovednosti jsou nezbytné
- Jsou vyžadovány disky, které lze přepínat mezi uzly klastru.
- Konfigurace klastrů s vysokou dostupností je poměrně složitá.
- Překonání selhání je historicky poměrně pomalé, ale nedávné produkty klastru s vysokou dostupností toto zlepšují.
- Nadbytečná překonání selhání se mohou vyskytnout, pokud existují nedostatky ve skriptech, které se používají k monitorování prostředků, jako jsou správci front.

Vztah klastrů HA ke klastrům správců front

Klastry správců front poskytují vyrovnávání zátěže zpráv v rámci dostupných instancí front klastru správců front. To nabízí vyšší dostupnost než jeden správce front, protože po selhání správce front mohou aplikace systému zpráv i nadále odesílat zprávy do přežívajících instancí fronty klastru správce front a přistupovat k nim. Ačkoli však klastry správců front automaticky směrují nové zprávy do dostupných správců front v klastru, zprávy aktuálně zařazené do fronty v nedostupném správci front nebudou k dispozici, dokud nebude tento správce front restartován. Z tohoto důvodu samotné klastry správců front neposkytují vysokou dostupnost všech dat zpráv ani neposkytují automatickou detekci selhání správce front a automatické spouštění restartování nebo překonání selhání správce front. Tyto funkce poskytují klastry s vysokou dostupností (HA). Tyto dva typy klastrů mohou být použity společně s dobrým efektem. Úvod do klastrů správců front naleznete v tématu Navrhování klastrů.

Související pojmy

Linux MQ Adv. CD Vysoká dostupnost pro IBM MQ Advanced container

Linux AIX Klastry HA na systému AIX and Linux

Produkt IBM MQ můžete použít s klastrem vysoké dostupnosti (HA) na platformách AIX and Linux : například PowerHA pro AIX (dříve HACMP), Veritas Cluster Server, HP Serviceguard nebo klastr Red Hat Enterprise Linux s Red Hat Cluster Suite.

Tento oddíl uvádí “Konfigurace klastru HA” na stránce 467, vztah klastrů s vysokou dostupností ke klastrům správců front, “IBM MQ klienti” na stránce 468a “IBM MQ pracující v klastru HA” na stránce 468a provádí vás kroky a poskytuje ukázkové skripty, které lze přizpůsobit konfiguraci správců front s klastrem s vysokou dostupností.

Chcete-li získat pomoc s kroky konfigurace popsanými v této sekci, prohlédněte si konkrétní dokumentaci klastru HA pro vaše prostředí.

Konfigurace klastru HA

V této části se výraz *uzel* používá k odkazování na entitu, na které je spuštěn operační systém a software HA; výraz "počítač", "systém" nebo "počítač" nebo "oblast" nebo "blade" může být v tomto použití považován za synonyma. Produkt IBM MQ můžete použít jako nápovědu pro nastavení konfigurace pohotovostního režimu nebo konfigurace převzetí, včetně vzájemného převzetí, kde jsou spuštěny všechny uzly klastru IBM MQ pracovní zátěže.

Konfigurace pohotovostního režimu je nejzákladnější konfigurace klastru vysoké dostupnosti, ve které jeden uzel provádí práci, zatímco druhý uzel pracuje pouze jako záložní. Pohotovostní uzel neprovádí práci a označuje se jako nečinný; tato konfigurace se někdy nazývá *studený pohotovostní režim*. Taková konfigurace vyžaduje vysoký stupeň redundance hardwaru. Chcete-li ušetřit na hardwaru, je možné rozšířit tuto konfiguraci tak, aby měla více pracovních uzlů s jedním rezervním uzlem. Jedná se o to, že záložní uzel může převzít práci libovolného jiného pracovního uzlu. Na tuto konfiguraci se stále odkazuje jako na pohotovostní konfiguraci a někdy jako na konfiguraci "N+1".

Konfigurace *převzetí* je pokročilejší konfigurace, ve které všechny uzly provádějí určitou práci a kritickou práci lze převzít v případě selhání uzlu.

Jednostranná konfigurace převzetí je konfigurace, ve které záložní uzel provádí další, nekritickou a nepohyblivou práci. Tato konfigurace je podobná konfiguraci v pohotovostním režimu, ale s (nekritickou) prací prováděnou záložním uzlem.

Konfigurace *vzájemného převzetí* je konfigurace, ve které všechny uzly provádějí vysoce dostupnou (pohyblivou) práci. Tento typ konfigurace klastru vysoké dostupnosti je také někdy označován jako "Aktivní/Aktivní", což označuje, že všechny uzly aktivně zpracovávají kritickou pracovní zátěž.

S rozšířenou konfigurací pohotovostního režimu nebo s některou z konfigurací převzetí je důležité zvážit maximální zátěž, kterou lze umístit na uzel, který může převzít práci jiných uzlů. Takový uzel musí mít dostatečnou kapacitu pro udržení přijatelné úrovně výkonu.

Vztah klastrů HA ke klastrům správců front

Klastry správců front omezují administraci a zajišťují vyrovnávání zátěže zpráv v rámci instancí front klastrů správců front. Nabízejí také vyšší dostupnost než jeden správce front, protože po selhání správce front mohou aplikace systému zpráv nadále přistupovat k přežívajícím instancím fronty klastru správce front. Samotné klastry správců front však neposkytují automatickou detekci selhání správce front a automatické spouštění restartování nebo překonání selhání správce front. Klastry HA poskytují tyto funkce. Tyto dva typy klastrů mohou být použity společně s dobrým efektem.

IBM MQ klienti

Klienti IBM MQ , kteří komunikují se správcem front, který může být restartován nebo převzat, musí být zapsáni, aby tolerovali přerušené připojení, a musí se opakovaně pokoušet o opětovné připojení. Produkt IBM MQzahrnuje funkce zpracování tabulky CCDT (Client Channel Definition Table), které pomáhají s dostupností připojení a vyrovnáváním pracovní zátěže. Tyto funkce však nejsou přímo relevantní při práci se systémem překonání selhání.

Funkce transakcí umožňuje produktu IBM MQ MQI client účastnit se dvoufázových transakcí, pokud je klient připojen ke stejnému správci front. Funkce transakcí nemohou k výběru ze seznamu správců front používat techniky, například prostředek pro vyrovnávání zátěže IP. Při použití produktu s vysokou dostupností si správce front uchovává svou identitu (název a adresu) bez ohledu na uzel, na kterém je spuštěn, takže transakční funkce lze používat se správci front, kteří jsou pod kontrolou vysoké dostupnosti.

IBM MQ pracující v klastru HA

Všechny klastry HA mají koncepci jednotky překonání selhání. Jedná se o sadu definic, která obsahuje všechny prostředky, které tvoří službu s vysokou dostupností. Jednotka překonání selhání zahrnuje samotnou službu a všechny ostatní prostředky, na kterých závisí.

Řešení HA používají různé termíny pro jednotku překonání selhání:

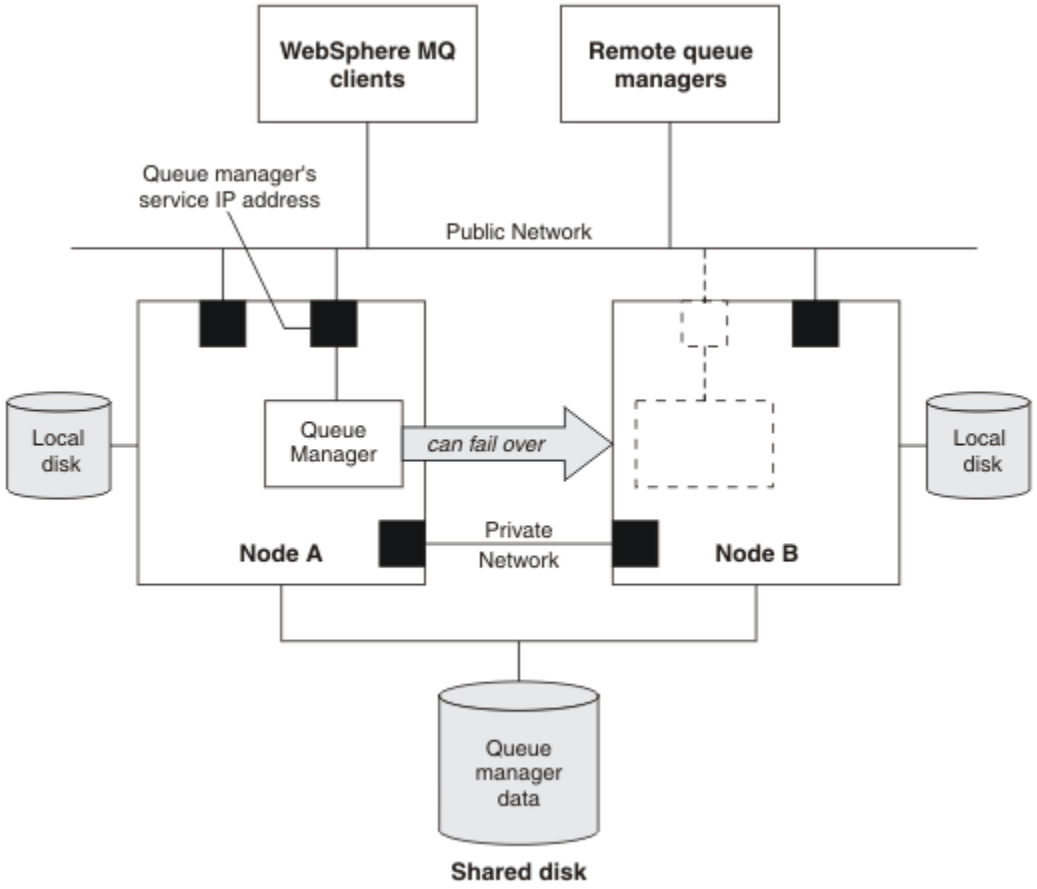
- V systému PowerHA for AIX se jednotka překonání selhání nazývá *skupina prostředků*.
- Na serveru Veritas Cluster Server se nazývá *skupina služeb*.
- Na Serviceguard se nazývá *balík*.

Toto téma používá termín *skupina prostředků* k označení jednotky překonání selhání.

Nejmenší jednotkou překonání selhání pro produkt IBM MQ je správce front. Skupina prostředků obsahující správce front obvykle obsahuje také sdílené disky ve skupině disků nebo skupině disků, které jsou vyhrazeny výhradně pro použití skupinou prostředků, a adresu IP, která se používá pro připojení ke správci front. Je také možné zahrnout další prostředky IBM MQ , jako např. modul listener nebo monitor spouštěčů, do stejné skupiny prostředků, buď jako samostatné prostředky, nebo pod řízení samotného správce front.

Správce front, který má být použit v klastru vysoké dostupnosti, musí mít svá data a protokoly na discích sdílených mezi uzly v klastru. Klastr HA zajišťuje, že na disky může v daném okamžiku zapisovat pouze jeden uzel v klastru. Klastr HA může použít skript monitoru k monitorování stavu správce front.

Pro data i protokoly související se správcem front lze použít jeden sdílený disk. Je však běžné používat oddělené sdílené systémy souborů, aby mohly být nezávisle dimenzovány a vyladěny.



Obrázek 69. Klastr HA

Obrázek 1 znázorňuje klastr s vysokou dostupností se dvěma uzly. Klastr s vysokou dostupností spravuje dostupnost správce front, který byl definován ve skupině prostředků. Jedná se o konfiguraci aktivního/pasivního nebo studeného pohotovostního režimu, 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 také spravována klastrem vysoké dostupnosti. Správce front závisí na sdíleném disku a jeho servisní adrese IP. Pokud klastr s vysokou dostupností selže při přechodu správce front z uzlu A do uzlu B, přesune nejprve závislé prostředky správce front do uzlu B a poté spustí správce front.

Pokud klastr s vysokou dostupností obsahuje více než jednoho správce front, může konfigurace klastru s vysokou dostupností po překonání selhání vést ke spuštění dvou nebo více správců front ve stejném uzlu. Každému správci front v klastru s vysokou dostupností musí být přiřazeno vlastní číslo portu, které používá v libovolném uzlu klastru, který je v daném okamžiku aktivní.

Obecně platí, že klastr HA je spuštěn jako uživatel root. Produkt IBM MQ se spouští jako uživatel mqm. Administrace produktu IBM MQ je udělena členům skupiny mqm. Ujistěte se, že uživatel mqm i skupina existují na všech uzlech klastru HA. ID uživatele a ID skupiny musí být v rámci klastru konzistentní. Administrace produktu IBM MQ uživatelem root není povolena; skripty, které spouštějí, zastavují nebo monitorují skripty, se musí přepnout na uživatele mqm.

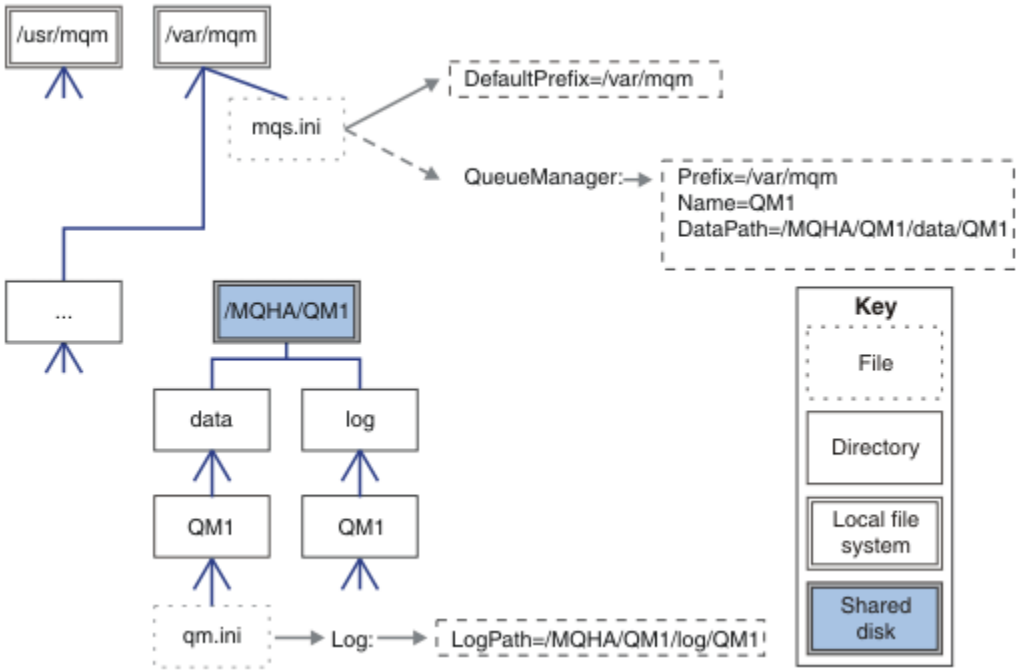
Poznámka: Produkt IBM MQ musí být správně nainstalován na všech uzlech; nemůžete sdílet spustitelné soubory produktu.

Linux AIX *Konfigurace sdílených disků v systému AIX and Linux*

Správce front IBM MQ v klastru vysoké dostupnosti vyžaduje, aby datové soubory a soubory protokolu byly ve společných pojmenovaných vzdálených systémech souborů na sdíleném disku.

Informace o této úloze

Obrázek 1 ukazuje možné rozvržení pro správce front v klastru s vysokou dostupností. Adresáře dat a protokolů správce front jsou na sdíleném disku, který je připojen v adresáři /MQHA/QM1. Tento disk se při překonání selhání přepíná mezi uzly klastru vysoké dostupnosti, aby byla data k dispozici při každém restartování správce front. Soubor `mqs.ini` obsahuje sekci pro správce front QM1 . Sekce Protokol v souboru `qm.ini` má hodnotu pro LogPath.



Obrázek 70. Sdílené adresáře `data` a `log`

Postup

1. Rozhodněte se o názvech bodů připojení pro systémy souborů správce front.

   Například `/MQHA/qmgrname/data` pro datové soubory správce front a `/MQHA/qmgrname/log` pro 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 disků.
4. Pro každý uzel vytvořte body připojení pro systémy souborů a ujistěte se, že lze systémy souborů připojit.

   Uživatel mqm musí vlastnit body připojení.

Linux AIX *Vytvoření správce front klastru HA v systému AIX and Linux*

Prvním krokem k použití správce front v klastru s vysokou dostupností je vytvoření správce front v jednom z uzlů.

Informace o této úloze

Chcete-li vytvořit správce front pro použití v klastru s vysokou dostupností, je třeba nejprve vybrat jeden z uzlů v klastru, v němž má být správce front vytvořen, a poté v tomto uzlu provést následující kroky.

Postup

1. Připojte systémy souborů správce front k 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 počáteční konfiguraci správce front, například vytvoření front a kanálů, a nastavte správce front tak, aby spustil modul listener automaticky při spuštění správce front.
5. Zastavte správce front pomocí příkazu **endmqm** .
6. Příkaz **dspmqinf** použijte k zobrazení příkazu **addmqinf** :

   ```
   dspmqinf -o command qmgrname
   ```

   kde `qmgrname` je název správce front.

   Další informace o použití příkazu **addmqinf** viz “Přidání konfigurace správce front do jiných uzlů klastru vysoké dostupnosti v systému AIX and Linux” na stránce 471.

   Příkaz **addmqinf** se zobrazí podobným způsobem jako v následujícím příkladu:

   ```
   addmqinf -sQueueManager -vName=qmgrname -vDirectory=qmgrname \
   -vPrefix=/var/mqm -vDataPath=/MQHA/qmgrname/data/qmgrname
   ```
7. Pečlivě si poznamenejte zobrazený příkaz.
8. Odpojte systémy souborů správce front.

Jak pokračovat dále

Nyní jste připraveni provést kroky popsané v tématu “Přidání konfigurace správce front do jiných uzlů klastru vysoké dostupnosti v systému AIX and Linux” na stránce 471.

Linux AIX *Přidání konfigurace správce front do jiných uzlů klastru vysoké dostupnosti v systému AIX and Linux*

Musíte přidat informace o konfiguraci správce front do ostatních uzlů v klastru vysoké dostupnosti.

Než začnete

Než dokončíte tuto úlohu, musíte dokončit kroky v části “Vytvoření správce front klastru HA v systému AIX and Linux” na stránce 470. Po vytvoření správce front je třeba přidat informace o konfiguraci správce front do všech ostatních uzlů v klastru vysoké dostupnosti provedením následujících kroků v každém z ostatních uzlů.

Informace o této úloze

Při vytváření správce front pro použití v klastru s vysokou dostupností je třeba nejprve vybrat jeden z uzlů v klastru, v němž má být vytvořen správce front, jak je popsáno v tématu “Vytvoření správce front klastru HA v systému AIX and Linux” na stránce 470.

Postup

1. Připojte systémy souborů správce front.
2. Přidejte do uzlu informace o konfiguraci správce front.
   Existují dva způsoby přidání informací o konfiguraci:
   - Přímou úpravou souboru `/var/mqm/mqs.ini` .

- Zadáním příkazu **addmqinf** , který byl zobrazen příkazem **dspmqinf** v kroku 6 v souboru “Vytvoření správce front klastru HA v systému AIX and Linux” na stránce 470.

3. Spusťte a zastavte správce front, abyste ověřili konfiguraci.

   Příkazy použité ke spuštění a zastavení správce front musí být zadány ze stejné instalace produktu IBM MQ jako příkaz **addmqinf** . Chcete-li spustit a zastavit správce front z jiné instalace, než je ta, která je aktuálně přidružena ke správci front, musíte nejprve nastavit instalaci přidruženou ke správci front pomocí příkazu **setmqm** . Další informace viz setmqm.
4. Odpojte systémy souborů správce front.

Linux AIX *Příklad skriptů shellu pro spuštění správce front klastru HA v systému AIX and Linux*

Správce front je v klastru HA reprezentován jako prostředek. Klastr HA 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, buď pomocí síťového systému souborů, nebo jejich zkopírováním na každý z lokálních disků.

Poznámka: Před restartováním nezdařeného správce front je nutné odpojit aplikace od této instance správce front. Pokud tak neučiníte, nemusí být správce front správně restartován.

Zde jsou uvedeny příklady vhodných skriptů shellu. Můžete je přizpůsobit vašim potřebám a použít je ke spuštění správce front pod kontrolou klastru vysoké dostupnosti.

Následující skript shellu je příkladem toho, jak přepnout z uživatele klastru HA na uživatele mqm, aby bylo možné úspěšně spustit správce front:

```
#!/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 náhlou metodu ukončení všech procesů, které patří do správce 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 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}
```

Skript můžete upravit tak, aby se spustily další související programy.

Linux AIX *Příklad skriptu shellu pro zastavení správce front klastru HA v systému AIX and Linux*

Ve většině případů můžete pomocí skriptu shellu zastavit správce front. Zde jsou uvedeny příklady vhodných skriptů shellu. Můžete je přizpůsobit svým potřebám a použít je k zastavení správce front pod kontrolou klastru vysoké dostupnosti.

Následující skript je příkladem toho, jak okamžitě zastavit správce front bez předpokladů o aktuálním stavu správce front. Skript musí být spuštěn uživatelem mqm. Proto může být nezbytné zabalit tento skript do skriptu shellu pro přepnutí uživatele z uživatele klastru HA na mqm. (Příklad skriptu shellu je uveden v souboru "Příklad skriptů shellu pro spuštění správce front klastru HA v systému AIX and Linux" na stránce 472.)

```
#!/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 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
```

Poznámka: V závislosti na spuštěných procesech pro specifického správce front nemusí být seznam procesů správce front obsažený v tomto skriptu úplným seznamem nebo může obsahovat více procesů, než jsou procesy spuštěné pro daného správce front:

```
for process in amqzmuc0 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
               amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
               amqzfuma amqzmuf0 amqzmur0 amqzmgr0
```

Proces lze zahrnout nebo vyloučit z tohoto seznamu na základě toho, která funkce je konfigurována a jaké procesy jsou spuštěny pro specifického správce front. Úplný seznam procesů a informace o zastavení procesů ve specifickém pořadí naleznete v tématu Ruční zastavení správce front v systémech UNIX a Linux.

Linux AIX *Monitorování správce front klastru HA v systému AIX and Linux*

Obvykle se jedná o způsob, jak může klastr s vysokou dostupností (HA) pravidelně monitorovat stav správce front. Ve většině případů k tomu můžete použít skript shellu. Zde jsou uvedeny příklady vhodných skriptů shellu. Tyto skripty můžete přizpůsobit svým potřebám a použít je k provedení dalších kontrol monitorování specifických pro vaše prostředí.

Je možné, že v systému existuje více instalací produktu IBM MQ současně. Další informace o více instalacích naleznete v tématu Vícenásobné instalace. Pokud hodláte používat skript monitorování ve více instalacích, možná budete muset provést některé další kroky. Máte-li primární instalaci, nemusíte zadat *MQ_INSTALLATION_PATH* pro použití skriptu. Jinak postupujte takto, abyste se ujistili, že je *MQ_INSTALLATION_PATH* správně identifikován:

1. Pomocí příkazu **crtmqenv** z instalace produktu IBM MQ identifikujte správný soubor *MQ_INSTALLATION_PATH* pro správce front:

   ```
   crtmqenv -m qmname
   ```

   Tento příkaz vrátí správnou hodnotu *MQ_INSTALLATION_PATH* pro správce front určeného parametrem *qmname*.
2. Spusťte skript monitorování s příslušnými parametry *qmname* a *MQ_INSTALLATION_PATH* .

Poznámka: PowerHA for AIX neposkytuje způsob, jak do monitorovacího programu pro správce front zadat parametr. Pro každého správce front musíte vytvořit samostatný program monitorování, který

zapouzdří název správce front. Zde je příklad skriptu používaného 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 nepovinný parametr, který určuje cestu k instalaci produktu IBM MQ , ke kterému je přidružen správce front *qmname* .

Následující skript není robustní vzhledem k možnosti, že **runmqsc** uvázne. Klastry vysoké dostupnosti obvykle považují zavěšený skript monitorování za selhání a jsou pro tuto možnost samy robustní.

Skript však toleruje, že se správce front nachází ve stavu spuštění. Je to proto, že je běžné, že klastr s vysokou dostupností spustí monitorování správce front ihned po jeho spuštění. Některé klastry HA rozlišují mezi počáteční fází a spuštěnou fází pro prostředky, ale je nutné nakonfigurovat dobu trvání počáteční fáze. Vzhledem k tomu, že doba potřebná ke spuštění správce front závisí na množství práce, kterou musí provést, je těžké zvolit maximální dobu, kterou spuštění správce front zabere. Zvolíte-li hodnotu, která je příliš nízká, klastr s vysokou dostupností nesprávně předpokládá, že došlo k selhání správce front při nedokončeném spuštění. To by mohlo vést k nekonečné posloupnosti selhání.

Tento skript musí být spuštěn uživatelem mqm. Proto může být nezbytné zabalit tento skript do skriptu shellu, aby se uživatel přepne z uživatele klastru HA na uživatele mqm (příklad skriptu shellu je uveden v souboru “Příklad skriptů shellu pro spuštění správce front klastru HA v systému AIX and Linux” na stránce 472):

```
#!/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
```

Linux AIX *Umístění správce front pod řízení klastru vysoké dostupnosti (HA) v systému AIX and Linux*

Musíte nakonfigurovat správce front pod kontrolou klastru HA s adresou IP správce front a sdílenými disky.

Informace o této úloze

Chcete-li správce front dostat pod řízení klastru HA, musíte definovat skupinu prostředků, která bude obsahovat správce front a všechny jeho přidružené prostředky.

Postup

1. Vytvořte skupinu prostředků obsahující správce front, svazek nebo skupinu disků správce front a adresu IP správce front.

   Adresa IP je virtuální adresa IP, ne adresa IP počítače.
2. Ověřte, zda klastr HA správně přepíná prostředky mezi uzly klastru a zda je připraven řídit správce front.

Linux AIX *Odstranění správce front klastru HA v systému AIX and Linux*

Možná budete chtít odebrat správce front z uzlu, který již není nutný pro spuštění správce front.

Informace o této úloze

Chcete-li odebrat správce front z uzlu v klastru HA, musíte odebrat jeho informace o konfiguraci.

Postup

1. Odeberte uzel z klastru HA, aby se klastr HA již nepokoušel aktivovat správce front v tomto uzlu.
2. Pomocí následujícího příkazu **rmvmqinf** odeberte informace o konfiguraci správce front:

   ```
   rmvmqinf qmgrname
   ```
3. Volitelné: Chcete-li zcela odstranit správce front, použijte příkaz **dltmqm** .

   Důležité: Mějte na paměti, že při odstranění správce front pomocí příkazu **dltmqm** dojde k úplnému odstranění dat a souborů protokolu správce front.

   Po odstranění správce front můžete pomocí příkazu **rmvmqinf** odebrat zbývající informace o konfiguraci z ostatních uzlů.

Windows Podpora Microsoft Cluster Service (MSCS)

Představení a nastavení MSCS pro podporu překonání selhání virtuálních serverů. MSCS je také známý jako Windows Server Failover Clustering (WSFC).

Tyto informace platí pouze pro IBM MQ for Windows .

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

MSCS/WSFC umožňuje připojit servery ke klastru, poskytuje vyšší dostupnost dat a aplikací a usnadňuje správu systému. MSCS/WSFC může automaticky detekovat a zotavit se ze selhání serveru nebo aplikace.

MSCS/WSFC podporuje překonání selhání virtuálních serverů, které odpovídají aplikacím, webům, tiskovým frontám nebo sdíleným souborům (včetně například jejich diskových vřeten, souborů a IP adres).

Překonání selhání je proces, při kterém produkt MSCS/WSFC zjistí selhání aplikace v jednom počítači v klastru a řádně ukončí přerušenou aplikaci, přenese její stavová data do jiného počítače a znovu tam zahájí aplikaci.

Informace o konfiguraci a použití clusterů s podporou převzetí služeb při selhání naleznete v dílčích tématech.

Windows *Představujeme klastry MSCS*

Klastry Microsoft Cluster Service (MSCS) jsou skupiny dvou nebo více počítačů, které jsou vzájemně propojeny a nakonfigurovány tak, že pokud jeden selže, provede MSCS *překonání selhání*, přenese data stavu aplikací z počítače, který selhal, do jiného počítače v klastru a znovu zahájí svou činnost.

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

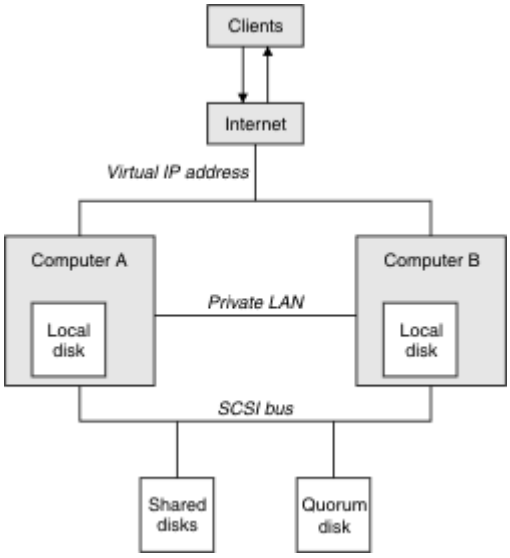
“Konfigurace vysoké dostupnosti” na stránce 465 obsahuje porovnání mezi klastry MSCS, správci front s více instancemi a klastry IBM MQ .

V této sekci a jejích podřízených tématech termín *klastr*, je-li použit samostatně, **vždy** znamená klastr MSCS. Liší se od klastru IBM 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 adresy IP*. Mohou být také vzájemně propojeny jednou nebo více soukromými sítěmi. A a B sdílí alespoň jeden disk pro serverové aplikace na každém z nich. K dispozici je také další sdílený disk, který musí být redundantní pole nezávislých disků (*RAID*). Úroveň 1, pro výhradní použití MSCS; označuje se jako disk *kvorum* . MSCS monitoruje oba počítače, aby zkontrolovala, zda hardware a software běží správně.

V jednoduchém nastavení, jako je tento, mají oba počítače všechny aplikace nainstalované na nich, ale pouze počítač A běží s živými aplikacemi; počítač B je právě spuštěn a čeká. Pokud počítač A narazí na některý z řady problémů, MSCS ukončí přerušenou aplikaci řádným způsobem, přenese její stavová data do jiného počítače a znovu tam zahájí aplikaci. Toto je známé jako *překonání selhání*. Aplikace lze nastavit *s ohledem na klastr* tak, aby plně komunikovaly s MSCS a s podporou převzetí služeb při selhání.

Typické nastavení pro klastr se dvěma počítači je uvedeno v části Obrázek 71 na stránce 477.



Obrázek 71. Klastr MSCS se dvěma počítači

Každý počítač může přistupovat ke sdílenému disku, ale pouze jeden po druhém, pod kontrolou MSCS. V případě překonání selhání přepne MSCS přístup k druhému počítači. Samotný sdílený disk je obvykle RAID, ale nemusí být.

Každý počítač je připojen k externí síti pro klientský přístup a každý má svou IP adresu. Externí klient, který komunikuje s tímto klastrem, si však uvědomuje pouze jednu *virtuální adresu IP*a MSCS správně směruje přenos IP v rámci klastru.

MSCS také provádí vlastní komunikaci mezi těmito dvěma počítači, buď přes jedno nebo více soukromých připojení, nebo přes veřejnou síť, například za účelem monitorování jejich stavů pomocí prezenčního signálu a synchronizace jejich databází.

Windows *Nastavení produktu IBM MQ pro klastrování MSCS*

Produkt IBM MQ nakonfigurujete pro klastrování tak, že ze správce front učiníte jednotku překonání selhání na MSCS. Správce front definujete jako prostředek MSCS, který jej pak může monitorovat, a v případě problému jej přenesete do jiného počítače v klastru.

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Chcete-li pro tento účel nastavit systém, začněte instalací produktu IBM MQ na každém počítači v klastru.

Vzhledem k tomu, že je správce front přidružen k názvu instalace produktu IBM MQ , měl by být název instalace produktu IBM MQ na všech počítačích v klastru stejný. Viz Instalace a odinstalace.

Sami správci front musí existovat pouze v počítači, ve kterém je vytváříte. V případě překonání selhání MSCS iniciuje 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 na lokální jednotce již nainstalovaného správce front, můžete jej migrovat pomocí nástroje poskytovaného s produktem IBM MQ; viz “Přesun správce front do úložiště MSCS” na stránce 480. Chcete-li vytvořit nové správce front pro použití s MSCS, postupujte podle části “Vytvoření správce front pro použití s MSCS” na stránce 480.

Po instalaci a migraci použijte administrátora klastru MSCS, abyste upozornili správce front na MSCS; viz “Vložení správce front pod řízení MSCS” na stránce 482.

Pokud se rozhodnete odebrat správce front z ovládacího prvku MSCS, použijte postup popsaný v části “Odebrání správce front z ovládacího prvku MSCS” na stránce 488.

Windows *Nastavení symetrie a MSCS*

Když se aplikace přepne z jednoho uzlu na druhý, musí se chovat stejným způsobem, bez ohledu na uzel. Nejlepším způsobem, jak to zajistit, je, aby byla prostředí identická.

Je-li to možné, nastavte klastr s identickým hardwarem, softwarem operačního systému, softwarem produktu a konfigurací na každém počítači. Zejména se ujistěte, že veškerý požadovaný software nainstalovaný na obou počítačích je identický, pokud jde o verzi, úroveň údržby, SupportPacs, cesty a uživatelské procedury, a že existuje společný obor názvů (prostředí zabezpečení), jak je popsáno v tématu “Zabezpečení MSCS” na stránce 478.

Windows *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 společný obor názvů (prostředí zabezpečení) v rámci klastru.
- Vytvořte uzly členů klastru MSCS domény, ve které je uživatelský účet, který je *vlastníkem klastru* , doménovým účtem.
- Učiňte ostatní uživatelské účty v klastru také doménovými účty, aby byly k dispozici na obou uzlech. Jedná se o automatický případ, pokud již máte doménu a účty relevantní pro produkt IBM MQ jsou doménové účty. Pokud momentálně nemáte doménu, zvažte nastavení *minidomény* tak, aby vyhovovala

uzlům klastru a příslušným účtům. Vaším cílem je, aby váš klastr dvou počítačů vypadal jako jeden výpočetní prostředek.

Nezapomeňte, že účet, který je lokální pro jeden počítač, neexistuje na druhém počítači. I když vytvoříte účet se stejným názvem na druhém počítači, jeho identifikátor zabezpečení (SID) se liší, takže když je aplikace přesunuta do jiného uzlu, oprávnění na tomto uzlu neexistují.

Během překonání selhání nebo přesunu podpora produktu IBM MQ MSCS zajistí, aby všechny soubory obsahující objekty správce front měly v cílovém uzlu ekvivalentní oprávnění. Kód explicitně kontroluje, zda skupiny Administrators a mqm a účet SYSTEM mají úplnou kontrolu a zda má produkt `Everyone` přístup pro čtení ke starému uzlu, je toto oprávnění přidáno do cílového uzlu.

Ke spuštění služby IBM MQ můžete použít účet domény. Ujistěte se, že existuje v lokální skupině mqm na každém počítači v klastru.

Windows *Použití více správců front s MSCS*

Pokud v počítači spouštíte více než jednoho správce front, můžete zvolit jednu z těchto nastavení.

Nastavení jsou následující:

- Všichni správci front v jedné skupině. Dojde-li v této konfiguraci k problému s jakýmkoli správcem front, budou všichni správci front ve skupině převedeni na jiný počítač jako skupina.
- Jeden správce front v každé skupině. Dojde-li v této konfiguraci k problému se správcem front, dojde k selhání samotného správce front v jiném počítači, aniž by došlo k ovlivnění ostatních správců front.
- Směs prvních dvou nastavení.

Windows *Režimy klastru a MSCS*

Existují dva režimy, ve kterých můžete spustit systém klastru s operačním systémem IBM MQ on Windows: Aktivní/Pasivní nebo Aktivní/Aktivní.

Poznámka: Pokud používáte MSCS společně s transakčním serverem Microsoft (COM +), nemůžete použít režim Aktivní/Aktivní.

Aktivní/pasivní režim

V aktivním/pasivním režimu má počítač A spuštěnou aplikaci a počítač B je zálohován, používá se pouze tehdy, když MSCS zjistí problém.

Tento režim můžete použít pouze s jedním sdíleným diskem, ale pokud některá aplikace způsobí překonání selhání, **všechny** aplikace musí být přeneseny jako skupina (protože ke sdílenému disku může v daném okamžiku přistupovat pouze jeden počítač).

MSCS můžete nakonfigurovat pomocí A jako *upřednostňovaný* počítač. Poté, když byl počítač A opraven nebo vyměněn a pracuje správně znovu, MSCS to detekuje a automaticky přepne aplikaci zpět na počítač A.

Pokud spouštíte více než jednoho správce front, zvažte možnost použití samostatného sdíleného disku pro každého z nich. Poté vložte jednotlivé správce front do samostatné skupiny v MSCS. Tímto způsobem může kterýkoli správce front provést překonání selhání na jiný počítač, aniž by to ovlivnilo ostatní správce front.

Aktivní/aktivní režim

V aktivním/aktivním režimu mají počítače A i B spuštěné aplikace a skupiny na každém počítači jsou nastaveny tak, aby používaly druhý počítač jako zálohu. Pokud je na počítači A zjištěno selhání, MSCS přenese stavová data do počítače B a tam znovu zahájí aplikaci. počítač B pak spustí vlastní aplikaci a A je.

Pro toto nastavení potřebujete alespoň dva sdílené disky. Můžete nakonfigurovat MSCS s A jako upřednostňovaným počítačem pro aplikace A a B jako upřednostňovaným počítačem pro aplikace B. Po překonání selhání a opravě každá aplikace automaticky skončí zpět na svém vlastním počítači.

V případě operačního systému IBM MQ to znamená, že můžete například spustit dva správce front, jednoho na každém z nich A a B, přičemž každý z nich bude využívat plný výkon svého vlastního počítače. Po selhání v počítači A budou oba správci front spuštění v počítači B. To bude znamenat sdílení výkonu jednoho počítače, se sníženou schopností zpracovávat velké množství dat rychlostí. Nicméně, vaše kritické aplikace budou stále k dispozici, zatímco zjistíte a opravíte poruchu na A.

Windows *Vytvoření správce front pro použití s MSCS*

Tento postup zajistí, že bude vytvořen nový správce front tak, aby byl vhodný pro přípravu a umístění pod řízení produktu Microsoft Cluster Service (MSCS).

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Nejprve vytvořte správce front se všemi jeho prostředky na lokální jednotce a poté migrujte soubory protokolu a datové soubory na sdílený disk. (Tuto operaci můžete zvrátit.) **Nepokoušejte se** vytvořit správce front s jeho prostředky na sdílené jednotce.

Správce front pro použití s MSCS můžete vytvořit dvěma způsoby, buď z příkazového řádku, nebo v adresáři IBM MQ Explorer. Výhodou použití příkazového řádku je, že správce front je vytvořen *zastavený* a nastaven na *ruční spuštění*, které je připraveno pro MSCS. (Produkt IBM MQ Explorer 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 s MSCS, postupujte takto:

1. Ujistěte se, že máte proměnnou prostředí `MQSPREFIX` nastavenou tak, aby odkazovala na lokální jednotku, například `C:\IBM MQ`. Pokud toto změníte, restartujte počítač, aby systémový účet změnu vyzvedl. Pokud proměnnou nenastavíte, bude správce front vytvořen ve výchozím adresáři IBM MQ pro správce front.
2. Vytvořte správce front pomocí příkazu **crtmqm** . Chcete-li například vytvořit správce front s názvem `mscs_test` ve výchozím adresáři, použijte:

   ```
   crtmqm mscs_test
   ```

3. Pokračujte na “Přesun správce front do úložiště MSCS” na stránce 480.

Vytvoření správce front pomocí konzoly IBM MQ Explorer

Chcete-li vytvořit správce front pomocí konzoly IBM MQ Explorerpro použití s MSCS, postupujte takto:

1. Spusťte IBM MQ Explorer z nabídky Start.
2. V pohledu Navigator rozbalte uzel stromu a vyhledejte uzel stromu `Správci front` .
3. Klepněte pravým tlačítkem myši na uzel stromu `Správci front` a vyberte volbu**Nový** > **Správce front**. Zobrazí se panel Vytvořit správce front.
4. Dokončete dialogové okno (krok 1) a poté klepněte na tlačítko **Další >**.
5. Dokončete dialogové okno (Krok 2) a poté klepněte na tlačítko **Další >**.
6. Dokončete dialogové okno (Krok 3) a ujistěte se, že nejsou vybrány volby `Spustit správce front` a `Vytvořit kanál připojení serveru` , poté klepněte na tlačítko **Další >**.
7. Dokončete dialogové okno (Krok 4) a poté klepněte na tlačítko **Dokončit**.
8. Pokračujte na “Přesun správce front do úložiště MSCS” na stránce 480.

Windows *Přesun správce front do úložiště MSCS*

Tento postup konfiguruje existujícího správce front tak, aby byl vhodný pro umístění pod řízení produktu Microsoft Cluster Service (MSCS).

Chcete-li toho dosáhnout, přesuňte soubory protokolu a datové soubory na sdílené disky, abyste je zpřístupnili druhému počítači v případě selhání. Existující správce front může mít například cesty jako `C:\WebSphere MQ\log\`*QMname* a `C:\WebSphere MQ\qmgrs\`*QMname*.

Upozornění: Nepokoušejte se přesunout soubory ručně; použijte obslužný program dodaný jako součást podpory IBM MQ MSCS, jak je popsáno v tomto tématu.

Pokud přesouvaný správce front používá připojení TLS a úložiště klíčů TLS se nachází v datovém adresáři správce front v lokálním počítači, bude úložiště klíčů přesunuto spolu se zbytkem správce front na sdílený disk. Standardně je atribut správce front, který určuje umístění úložiště klíčů TLS, SSLKEYR, nastaven na hodnotu *MQ_INSTALLATION_PATH*`\qmgrs\QMGRNAME\ssl\key`, která se nachází v datovém adresáři správce front. *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ . Příkaz `hamvmqm` neupravuje tento atribut správce front. V této situaci musíte upravit atribut správce front SSLKEYR pomocí příkazu IBM MQ Explorer nebo MQSC `ALTER QMGR`tak, aby ukazoval na nový soubor úložiště klíčů TLS.

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Postup je následující:

1. Ukončete práci správce front a zkontrolujte, zda nedošlo k žádným chybám.
2. Pokud jsou soubory protokolu nebo soubory fronty správce front již uloženy na sdíleném disku, přeskočte zbytek tohoto postupu a pokračujte přímo na “Vložení správce front pod řízení MSCS” na stránce 482.
3. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (viz “Soubory protokolu správce front” na stránce 491 , proč je to důležité).
4. Pokud již máte vhodný prostředek sdíleného disku, pokračujte krokem 6. Jinak pomocí administrátora klastru MSCS vytvořte prostředek typu *sdílený disk* s dostatečnou kapacitou pro uložení souborů protokolu a datových souborů (front) správce front.
5. Otestujte sdílený disk pomocí administrátora klastru MSCS, abyste jej přesunuli z jednoho uzlu klastru na druhý a znovu.
6. Ujistěte se, že sdílený disk je online na uzlu klastru, kde jsou lokálně uloženy protokoly správce front a datové soubory.
7. Spuštěním obslužného programu přesuňte správce front následujícím způsobem:

   ```
   hamvmqm /m qmname /dd " e: \
   IBM MQ " /ld " e: \
   IBM MQ \log"
   ```

   nahrazení názvu správce front názvem *qmname*, písmenem sdílené diskové jednotky *e*a zvoleným adresářem produktu *IBM MQ*. Adresáře se vytvoří, pokud ještě neexistují.
8. Otestujte správce front, abyste se ujistili, že funguje, pomocí konzoly IBM MQ Explorer. Příklad:
   a. Klepněte pravým tlačítkem myši na uzel stromu správce front a vyberte volbu **Spustit**. Spustí se správce front.
   b. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a vyberte volbu **Nová** > **Lokální fronta ...**, a pojmenujte frontu.
   c. Klepněte na tlačítko **Dokončit**.
   d. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel Vložit testovací zprávu.
   e. Zadejte text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.
   f. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Procházet zprávy ...**. Zobrazí se panel Prohlížeč zpráv.
   g. Zkontrolujte, zda je zpráva ve frontě, a poté klepněte na tlačítko **Zavřít**. Panel Prohlížeč zpráv se zavře.

h. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.

i. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Odstranit ...**. Zobrazí se potvrzovací panel, klepněte na tlačítko **OK**. Fronta je odstraněna.

j. Klepněte pravým tlačítkem myši na uzel stromu správce front a vyberte volbu **Zastavit ...**. Zobrazí se panel Ukončit správce front.

k. Klepněte na tlačítko **OK**. Správce front se zastaví.

9. Jako administrátor systému IBM MQ se ujistěte, že atribut spuštění správce front je nastaven na ruční. V souboru IBM MQ Explorernastavte pole Spuštění na hodnotu `manual` na panelu vlastností správce front.
10. Pokračujte na "Vložení správce front pod řízení MSCS" na stránce 482.

Windows *Vložení správce front pod řízení MSCS*

Jak umístit správce front pod řízení produktu Microsoft Cluster Service (MSCS), včetně předem požadovaných úloh.

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Před vložením správce front pod řízení MSCS/WSFC

Před vložením správce front pod řízení MSCS/WSFC postupujte takto:

1. Ujistěte se, že produkt IBM MQ a jeho podpora MSCS/WSFC jsou nainstalovány na obou počítačích v klastru a že software na každém počítači je identický, jak je popsáno v tématu "Nastavení produktu IBM MQ pro klastrování MSCS" na stránce 478.
2. Obslužný program **haregtyp** použijte k registraci IBM MQ jako typ prostředku MSCS na všech uzlech klastru. Viz téma "Podpora obslužných programů MSCS" na stránce 492.
3. Pokud jste tak dosud neučinili, vytvořte správce front pro použití s MSCS/WSFC.
4. Pokud jste vytvořili správce front nebo již existuje, ujistěte se, že jste provedli proceduru v adresáři "Přesun správce front do úložiště MSCS" na stránce 480.
5. Pokud je správce front spuštěn, zastavte jej pomocí příkazového řádku nebo Průzkumníku IBM MQ .
6. Otestujte operaci MSCS/WSFC sdílených jednotek před tím, než začnete s některou z následujících procedur Windows v tomto tématu.

Windows Server 2012, 2016, 2019 nebo 2022

Chcete-li umístit správce front pod řízení MSCS/WSFC na serveru Windows Server 2012 nebo novější, 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 pro správu clusteru s podporou převzetí služeb při selhání.
3. Klepněte pravým tlačítkem myši na volbu **Správa clusteru s podporou převzetí služeb při selhání > Připojit cluster ...** chcete-li otevřít připojení ke klastru.
4. Na rozdíl od skupinového schématu používaného v nástroji MSCS Cluster Administrator v předchozích verzích produktu Windowspoužívá nástroj pro správu clusteru s podporou převzetí služeb při selhání koncepci služeb a aplikací. Nakonfigurovaná služba nebo aplikace obsahuje všechny prostředky nezbytné pro klastrování jedné aplikace. Správce front můžete konfigurovat pod WSFC následujícím způsobem:

   a. Klepněte pravým tlačítkem myši na klastr a vyberte volbu **Konfigurovat roli** , abyste spustili průvodce konfigurací.

   b. Na panelu "Vybrat službu nebo aplikaci" vyberte volbu **Jiný server** .

c. Vyberte odpovídající adresu IP jako přístupový bod klienta.

   Tato adresa by měla být nevyužitou adresou IP, kterou mají používat klienti a jiní správci front pro připojení k *virtuálnímu* správci front. Tato adresa IP není normální (statická) adresou ani jednoho z uzlů; jedná se o další adresu, mezi kterou jsou *plovoucí* . Ačkoli adaptér WSFC 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 jej bude možné přiřadit.

   Můžete použít jednu jednotku k uložení protokolů i souborů fronty, nebo je můžete rozdělit na jednotky. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, zkontrolujte, zda jsou všechny jednotky používané tímto správcem front výlučné pro tohoto správce front, tj. že na jednotkách již nic jiného nespoléhá. Také se ujistěte, že jste vytvořili instanci prostředku pro každou jednotku, kterou používá správce front.

   Typ prostředku pro jednotku závisí na používané podpoře SCSI. Prostudujte si pokyny k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte jej z aktuální skupiny do skupiny vytvořené pro správce front.

   Pro každý prostředek jednotky nastavte možné vlastníky na oba uzly. Nastavte závislé prostředky na hodnotu none.

e. Vyberte prostředek **MQSeries MSCS** na panelu "Vybrat typ prostředku".

f. Dokončete zbývající kroky v průvodci.

5. Před uvedením prostředku do stavu online potřebuje prostředek MQSeries MSCS další konfiguraci:

   a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'New MQSeries MSCS'.

   b. Klepněte pravým tlačítkem myši na volbu **Vlastnosti** v prostředku MQ .

   c. Nakonfigurujte prostředek:

   - `Name` ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
   - `Run in a separate Resource Monitor` ; pro lepší izolaci
   - `Possible owners` ; nastavit oba uzly
   - `Dependencies` ; Přidejte jednotku a adresu IP pro tohoto správce front.

     Varování: Selhání přidání těchto závislostí znamená, že produkt IBM MQ se během překonání selhání pokusí zapsat stav správce front na chybný disk klastru. Vzhledem k tomu, že mnoho procesů se může pokoušet zapisovat na tento disk současně, některé procesy IBM MQ mohou být blokovány.

   - `Parameters` ; následujícím způsobem:
     – `QueueManagerName` (povinné); název správce front, který má tento prostředek řídit. Tento správce front musí existovat v lokálním počítači.
     – `PostOnlineCommand` (volitelné); můžete určit program, který má být spuštěn vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz “Příkaz PostOnlinea příkaz PreOfflinev MSCS” na stránce 491.
     – `PreOfflineCommand` (volitelné); můžete určit program, který se má spustit, kdykoli prostředek správce front změní svůj stav z online na offline. Další podrobnosti viz “Příkaz PostOnlinea příkaz PreOfflinev MSCS” na stránce 491.

       Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 60000 ms. Tato výchozí nastavení lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz “looksAlive a isAlive systém výzev na MSCS” na stránce 488.

   d. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v části “Použití upřednostňovaných uzlů v MSCS” na stránce 492).

e. *Zásada překonání selhání* je standardně nastavena na rozumné hodnoty, ale můžete vyladit prahové hodnoty a období, která řídí *Překonání selhání prostředku* a *Překonání selhání skupiny* tak, aby odpovídaly zátěžím umístěným ve správci front.

6. Otestujte správce front tak, že jej v produktu MSCS Cluster Administrator přivede do režimu online a podrobí jej testovací pracovní zátěži. Pokud experimentujete se správcem front testu, použijte Průzkumníka IBM MQ . Příklad:

   a. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a vyberte volbu **Nová** > **Lokální fronta ...**, a pojmenujte frontu.

   b. Klepněte na tlačítko **Dokončit**. Fronta je vytvořena a zobrazena v pohledu Obsah.

   c. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel Vložit testovací zprávu.

   d. Zadejte text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.

   e. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Procházet zprávy ...**. Zobrazí se panel Prohlížeč zpráv.

   f. Zkontrolujte, zda je zpráva ve frontě, a poté klepněte na tlačítko **Zavřít**. Panel Prohlížeč zpráv se zavře.

   g. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.

   h. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Odstranit ...**. Zobrazí se potvrzovací panel, klepněte na tlačítko **OK**. Fronta je odstraněna.

7. Pomocí administrátora klastru MSCS otestujte, zda lze správce front převést do režimu offline a zpět do režimu online.

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 jindy rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části “Přesun správce front do úložiště MSCS” na stránce 480.) Můžete také klepnout pravým tlačítkem myši a vybrat `Initiate Failure` ; akce (lokální restart nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows Server 2008

Chcete-li umístit správce front pod řízení MSCS na server 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 pro správu clusteru s podporou převzetí služeb při selhání.

3. Klepněte pravým tlačítkem myši na volbu **Správa clusteru s podporou převzetí služeb při selhání > Spravovat cluster ...** chcete-li otevřít připojení ke klastru.

4. Na rozdíl od skupinového schématu používaného v nástroji MSCS Cluster Administrator v předchozích verzích produktu Windowspoužívá nástroj pro správu clusteru s podporou převzetí služeb při selhání koncepci služeb a aplikací. Nakonfigurovaná služba nebo aplikace obsahuje všechny prostředky nezbytné pro klastrování jedné aplikace. Správce front můžete konfigurovat pod MSCS následujícím způsobem:

   a. Klepněte pravým tlačítkem myši na volbu **Služby a aplikace > Konfigurovat službu nebo aplikaci ...** ke spuštění průvodce konfigurací.

   b. Vyberte volbu **Jiný server** na panelu **Vybrat službu nebo aplikaci** .

   c. Vyberte odpovídající adresu IP jako přístupový bod klienta.

      Tato adresa by měla být nevyužitou adresou IP, kterou mají používat klienti a jiní správci front pro připojení k *virtuálnímu* správci front. Tato adresa IP není normální (statická) adresou ani jednoho

z uzlů; jedná se o další adresu, mezi kterou jsou *plovoucí* . Ačkoli 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 jej bude možné přiřadit.

Můžete použít jednu jednotku k uložení protokolů i souborů fronty, nebo je můžete rozdělit na jednotky. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, zkontrolujte, zda jsou všechny jednotky používané tímto správcem front výlučné pro tohoto správce front, tj. že na jednotkách již nic jiného nespoléhá. Také se ujistěte, že jste vytvořili instanci prostředku pro každou jednotku, kterou používá správce front.

Typ prostředku pro jednotku závisí na používané podpoře SCSI. Prostudujte si pokyny k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte jej z aktuální skupiny do skupiny vytvořené pro správce front.

Pro každý prostředek jednotky nastavte možné vlastníky na oba uzly. Nastavte závislé prostředky na hodnotu none.

e. Vyberte prostředek **MQSeries MSCS** na panelu **Vybrat typ prostředku** .

f. Dokončete zbývající kroky v průvodci.

5. Před uvedením prostředku do stavu online potřebuje prostředek MQSeries MSCS další konfiguraci:

a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'New MQSeries MSCS'.

b. Klepněte pravým tlačítkem myši na volbu **Vlastnosti** v prostředku MQ .

c. Nakonfigurujte prostředek:

- `Name` ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
- `Run in a separate Resource Monitor` ; pro lepší izolaci
- `Possible owners` ; nastavit oba uzly
- `Dependencies` ; Přidejte jednotku a adresu IP pro tohoto správce front.

  Varování: Selhání přidání těchto závislostí znamená, že produkt IBM MQ se během překonání selhání pokusí zapsat stav správce front na chybný disk klastru. Vzhledem k tomu, že mnoho procesů se může pokoušet zapisovat na tento disk současně, některé procesy IBM MQ mohou být blokovány.
- `Parameters` ; následujícím způsobem:
  - `QueueManagerName` (povinné); název správce front, který má tento prostředek řídit. Tento správce front musí existovat v lokálním počítači.
  - `PostOnlineCommand` (volitelné); můžete určit program, který má být spuštěn vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz “Příkaz PostOnlinea příkaz PreOfflinev MSCS” na stránce 491.
  - `PreOfflineCommand` (volitelné); můžete určit program, který se má spustit, kdykoli prostředek správce front změní svůj stav z online na offline. Další podrobnosti viz “Příkaz PostOnlinea příkaz PreOfflinev MSCS” na stránce 491.

    Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 60000 ms. Tato výchozí nastavení lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz “looksAlive a isAlive systém výzev na MSCS” na stránce 488.

d. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v části “Použití upřednostňovaných uzlů v MSCS” na stránce 492).

e. *Zásada překonání selhání* je standardně nastavena na rozumné hodnoty, ale můžete vyladit prahové hodnoty a období, která řídí *Překonání selhání prostředku* a *Překonání selhání skupiny* tak, aby odpovídaly zátěžím umístěným ve správci front.

6. Otestujte správce front tak, že jej v produktu MSCS Cluster Administrator přivede do režimu online a podrobí jej testovací pracovní zátěži. Pokud experimentujete se správcem front testu, použijte Průzkumníka IBM MQ . Příklad:
   a. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a vyberte volbu **Nová** > **Lokální fronta ...**, a pojmenujte frontu.
   b. Klepněte na tlačítko **Dokončit**. Fronta je vytvořena a zobrazena v pohledu Obsah.
   c. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel **Vložit testovací zprávu** .
   d. Zadejte text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.
   e. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Procházet zprávy ...**. Zobrazí se panel **Prohlížeč zpráv** .
   f. Zkontrolujte, zda je zpráva ve frontě, a poté klepněte na tlačítko **Zavřít**. Panel **Prohlížeč zpráv** se zavře.
   g. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.
   h. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Odstranit ...**. Zobrazí se potvrzovací panel, klepněte na tlačítko **OK**. Fronta je odstraněna.
7. Pomocí administrátora klastru MSCS otestujte, zda lze správce front převést do režimu offline a zpět do režimu online.
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 jindy rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části “Přesun správce front do úložiště MSCS” na stránce 480.) Můžete také klepnout pravým tlačítkem myši a vybrat `Initiate Failure` ; akce (lokální restart nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows 2003

Chcete-li umístit správce front pod řízení MSCS v systému Windows 2003, 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 administrátora klastru MSCS.
3. Otevřete připojení ke klastru.
4. Vytvořte skupinu MSCS, která má obsahovat prostředky pro správce front. Pojmenujte skupinu tak, aby bylo zřejmé, ke kterému správci front se vztahuje. Každá skupina může obsahovat více správců front, jak je popsáno v tématu “Použití více správců front s MSCS” na stránce 479.

   Použijte skupinu pro všechny zbývající kroky.
5. Vytvořte instanci prostředku pro všechny logické jednotky SCSI, které správce front používá.

   Můžete použít jednu jednotku k uložení protokolů i souborů fronty, nebo je můžete rozdělit na jednotky. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, zkontrolujte, zda jsou všechny jednotky používané tímto správcem front výlučné pro tohoto správce front, tj. že na jednotkách již nic jiného nespoléhá. Také se ujistěte, že jste vytvořili instanci prostředku pro každou jednotku, kterou používá správce front.

   Typ prostředku pro jednotku závisí na používané podpoře SCSI. Prostudujte si pokyny k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte jej z aktuální skupiny do skupiny vytvořené pro správce front.

   Pro každý prostředek jednotky nastavte možné vlastníky na oba uzly. Nastavte závislé prostředky na hodnotu none.

6. Vytvořte instanci prostředku pro adresu IP.

   Vytvořte prostředek adresy IP (typ prostředku *Adresa IP*). Tato adresa by měla být nevyužitou adresou IP, kterou mají používat klienti a jiní správci front pro připojení k *virtuálnímu* správci front. Tato adresa IP není normální (statická) adresou ani jednoho z uzlů; jedná se o další adresu, mezi kterou jsou *plovoucí* . Ačkoli MSCS zpracovává směrování této adresy, **neověřuje** , zda je adresa dosažitelná.

7. Vytvořte instanci prostředku pro správce front.

   Vytvořte prostředek typu *IBM MQ MSCS*. Průvodce vás vyzve k zadání různých položek, včetně následujících:

   - `Name` ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
   - `Add to group` ; použijte skupinu, kterou jste vytvořili
   - `Run in a separate Resource Monitor` ; pro lepší izolaci
   - `Possible owners` ; nastavit oba uzly
   - `Dependencies` ; Přidejte jednotku a adresu IP pro tohoto správce front.

     Varování: Selhání přidání těchto závislostí znamená, že produkt IBM MQ se během překonání selhání pokusí zapsat stav správce front na chybný disk klastru. Vzhledem k tomu, že mnoho procesů se může pokoušet zapisovat na tento disk současně, některé procesy IBM MQ mohou být blokovány.
   - `Parameters` ; následujícím způsobem:
     - `QueueManagerName` (povinné); název správce front, který má tento prostředek řídit. Tento správce front musí existovat v lokálním počítači.
     - `PostOnlineCommand` (volitelné); můžete určit program, který má být spuštěn vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz "Příkaz PostOnlinea příkaz PreOfflinev MSCS" na stránce 491.
     - `PreOfflineCommand` (volitelné); můžete určit program, který se má spustit, kdykoli prostředek správce front změní svůj stav z online na offline. Další podrobnosti viz "Příkaz PostOnlinea příkaz PreOfflinev MSCS" na stránce 491.

       Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 30000 ms. Tato výchozí nastavení lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz "looksAlive a isAlive systém výzev na MSCS" na stránce 488.

8. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v části "Použití upřednostňovaných uzlů v MSCS" na stránce 492).
9. *Zásada překonání selhání* (jak je definováno ve vlastnostech skupiny) je standardně nastavena na rozumné hodnoty, ale můžete vyladit prahové hodnoty a období, která řídí *Překonání selhání prostředků* a *Překonání selhání skupiny* , aby odpovídaly zátěžím umístěným ve správci front.
10. Otestujte správce front tak, že jej v produktu MSCS Cluster Administrator přivede do režimu online a podrobí jej testovací pracovní zátěži. Pokud experimentujete se správcem front testu, použijte Průzkumníka IBM MQ . Příklad:

    a. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a vyberte volbu **Nová** > **Lokální fronta ...**, a pojmenujte frontu.

    b. Klepněte na tlačítko **Dokončit**. Fronta je vytvořena a zobrazena v pohledu Obsah.

    c. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel **Vložit testovací zprávu** .

    d. Zadejte text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.

    e. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Procházet zprávy ...**. Zobrazí se panel **Prohlížeč zpráv** .

    f. Zkontrolujte, zda je zpráva ve frontě, a poté klepněte na tlačítko **Zavřít**. Panel **Prohlížeč zpráv** se zavře.

g. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.

h. Klepněte pravým tlačítkem myši na frontu a vyberte volbu **Odstranit ...**. Zobrazí se potvrzovací panel, klepněte na tlačítko **OK**. Fronta je odstraněna.

11. Pomocí administrátora klastru MSCS otestujte, zda lze správce front převést do režimu offline a zpět do režimu online.
12. Simulovat překonání selhání.

    V administrátorovi klastru MSCS klepněte pravým tlačítkem myši na skupinu obsahující správce front a vyberte volbu `Move Group`. To může trvat několik minut. (Pokud chcete jindy rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části "Přesun správce front do úložiště MSCS" na stránce 480.) Můžete také klepnout pravým tlačítkem myši a vybrat `Initiate Failure` ; akce (lokální restart nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows *looksAlive a isAlive systém výzev na MSCS*

looksAlive a *isAlive* jsou intervaly, ve kterých Microsoft Cluster Service (MSCS) volá zpět do kódu knihovny dodaného s typy prostředků a požaduje, aby prostředek provedl kontroly, aby určil pracovní stav sám sebe. To nakonec určuje, zda se MSCS pokusí o překonání selhání prostředku.

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Při každém uplynutí intervalu *looksAlive* (výchozí hodnota je 5000 ms) je prostředek správce front volán, aby provedl vlastní kontrolu a zjistil, zda je jeho stav uspokojivý.

Pokaždé, když uplyne interval *isAlive* (výchozí hodnota je 30000 ms), provede se další volání prostředku správce front, aby se provedla další kontrola, která určí, zda prostředek správně funguje. To umožňuje dvě úrovně kontroly typu prostředku.

1. Kontrola stavu *looksAlive* , která zjišťuje, zda prostředek funguje.
2. Významnější kontrola *isAlive* , která určuje, zda je prostředek správce front aktivní.

Pokud je zjištěno, že prostředek správce front není aktivní, MSCS na základě jiných rozšířených voleb MSCS spustí překonání selhání pro prostředek a přidružené závislé prostředky do jiného uzlu v klastru. Další informace viz Dokumentace MSCS.

Windows *Odebrání správce front z ovládacího prvku MSCS*

Můžete odebrat správce front z ovládacího prvku Microsoft Cluster Service (MSCS) a vrátit je do ruční administrace.

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Není nutné odebírat správce front z řízení MSCS pro operace údržby. To lze provést přechodným přechodem správce front do režimu offline s použitím modulu MSCS Cluster Administrator. Odebrání správce front z ovládacího prvku MSCS je trvalejší změna; tuto změnu proveďte pouze v případě, že se rozhodnete, že již nechcete, aby MSCS mělo další řízení správce front.

Pokud odebíraný správce front používá připojení TSL, musíte upravit atribut správce front SSLKEYR pomocí IBM MQ Průzkumníka nebo příkazu MQSC `ALTER QMGR`tak, aby ukazoval na soubor úložiště klíčů TLS v lokálním adresáři.

Postup je následující:

1. Převeďte prostředek správce front do stavu offline pomocí administrátora klastru MSCS, jak je popsáno v tématu "Převedení správce front z MSCS do režimu offline" na stránce 489 .
2. Zničte instanci prostředku. Tím nedojde ke zničení správce front.
3. Volitelně můžete soubory správce front migrovat zpět ze sdílených jednotek na lokální jednotky. Chcete-li to provést, prohlédněte si téma "Vrácení správce front z úložiště MSCS" na stránce 489.
4. Otestujte správce front.

Převedení správce front z MSCS do režimu offline

Chcete-li převést správce front z MSCS do stavu offline, postupujte takto:

1. Spusťte administrátora klastru MSCS.
2. Otevřete připojení ke klastru.
3. Pokud používáte produkt Windows 2012, vyberte volbu `Groups`nebo `Role` a otevřete skupinu obsahující správce front, který má být přesunut.
4. Vyberte prostředek správce front.
5. Klepněte na něj pravým tlačítkem myši a vyberte `Offline`.
6. Počkejte na dokončení.

Vrácení správce front z úložiště MSCS

Tento postup konfiguruje správce front tak, aby byl zpět na lokální jednotce počítače, tj. aby se stal *normálním* IBM MQ správcem front. Chcete-li toho dosáhnout, přesuňte soubory protokolu a datové soubory ze sdílených disků. Existující správce front může mít například cesty jako `E:\WebSphere MQ\log\`*QMname* a `E:\WebSphere MQ\qmgrs\`*QMname*. Nepokoušejte se přesunout soubory ručně; použijte obslužný program **hamvmqm** dodaný jako součást podpory IBM MQ MSCS:

1. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (viz “Soubory protokolu správce front” na stránce 491 , proč je to důležité).
2. Rozhodněte, která lokální jednotka se má použít, a ujistěte se, že má dostatečnou kapacitu pro uložení souborů protokolu a souborů dat (front) správce front.
3. Ujistěte se, že sdílený disk, na kterém jsou soubory momentálně umístěny, je online v uzlu klastru, do kterého se mají přesunout soubory protokolu a datové soubory správce front.
4. Spuštěním obslužného programu přesuňte správce front následujícím způsobem:

   ```
   hamvmqm /m qmname /dd " c:\
   IBM MQ " /ld "c:\
   IBM MQ \log"
   ```

   nahrazení názvu správce front názvem *qmname*, písmenem lokální diskové jednotky *c*a zvoleným adresářem produktu *IBM MQ* (adresáře se vytvoří, pokud dosud neexistují).
5. Otestujte správce front, abyste se ujistili, že funguje (jak je popsáno v tématu “Přesun správce front do úložiště MSCS” na stránce 480).

Windows *Rady a tipy pro používání MSCS*

Tento oddíl obsahuje některé obecné informace, které vám pomohou efektivně používat IBM MQ podporu pro Microsoft Cluster Service (MSCS).

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Jak dlouho trvá selhání správce front z jednoho počítače na druhý? To silně závisí na množství pracovní zátěže ve správci front a na kombinaci provozu, například na tom, kolik z nich je trvalých, v synchronizačním bodě a kolik je potvrzeno před selháním. Testy produktu IBM mají k dispozici dobu překonání selhání a odvolání při selhání přibližně jednu minutu. Jednalo se o velmi lehce načteného správce front a skutečné časy se budou značně lišit v závislosti na zatížení.

Windows *Ověření, že MSCS funguje*

Chcete-li se ujistit, že máte spuštěný klastr MSCS, postupujte takto.

Popisy úloh začínající na “Vytvoření správce front pro použití s MSCS” na stránce 480 předpokládají, že máte spuštěný klastr MSCS, ve kterém můžete vytvářet, migrovat a likvidovat prostředky. Chcete-li se ujistit, že máte takový klastr:

1. Pomocí administrátora klastru MSCS vytvořte skupinu.

2. V rámci této skupiny vytvořte instanci prostředku generické aplikace s uvedením systémových hodin (název cesty `C:\winnt\system32\clock.exe` a pracovní adresář `C:\`).
3. Ujistěte se, že můžete prostředek převést do režimu online, že můžete přesunout skupinu, která jej obsahuje, do jiného uzlu a že můžete prostředek převést do režimu offline.

Windows *Ruční spuštění a MSCS*

Pro správce front spravovaného pomocí MSCS musíte nastavit atribut spuštění na ruční. Tím je zajištěno, že podpora IBM MQ MSCS může restartovat službu MQSeries bez okamžitému spuštění správce front.

Podpora IBM MQ MSCS musí být schopna restartovat službu, aby mohla provádět monitorování a řízení, ale sama musí mít kontrolu nad tím, kteří správci front jsou spuštěni a na kterých počítačích. Další informace viz “Přesun správce front do úložiště MSCS” na stránce 480.

Windows *MSCS a správci front*

Aspekty týkající se správců front při použití MSCS.

Vytvoření odpovídajícího správce front v jiném uzlu

Aby klastrování fungovalo s produktem IBM MQ, potřebujete identického správce front v uzlu B pro každý z nich v uzlu A. Druhou však nemusíte explicitně vytvářet. Můžete vytvořit nebo připravit správce front v jednom uzlu, přesunout jej do jiného uzlu, jak je popsáno v tématu “Přesun správce front do úložiště MSCS” na stránce 480, a v tomto uzlu je zcela duplikován.

Výchozí správci front

Nepoužívejte výchozího správce front pod řízením MSCS. Správce front nemá vlastnost, která by jej nastavila jako výchozí; produkt IBM MQ uchovává svůj vlastní samostatný záznam. Pokud přesunete správce front, který je nastaven jako výchozí, na jiný počítač při překonání selhání, nestane se výchozím. Zajistěte, aby všechny aplikace odkazovaly na konkrétní správce front podle názvu.

Odstranění správce front

Po přesunutí uzlu správcem front existují jeho podrobnosti v registru v obou počítačích. Chcete-li jej odstranit, proveďte to na jednom počítači jako obvykle a poté spusťte obslužný program popsaný v části “Podpora obslužných programů MSCS” na stránce 492 , abyste vyčistili registr na druhém počítači.

Podpora existujících správců front

Můžete umístit existujícího správce front pod řízení MSCS za předpokladu, že soubory protokolu a soubory front správce front můžete umístit na disk, který je mezi těmito dvěma počítači na sdílené sběrnici SCSI (viz Obrázek 71 na stránce 477). Při vytváření prostředku MSCS je třeba správce front krátce převést do stavu offline.

Chcete-li vytvořit nového správce front, vytvořte jej nezávisle na MSCS, otestujte jej a poté jej umístěte pod řízení MSCS. Viz:

- “Vytvoření správce front pro použití s MSCS” na stránce 480
- “Přesun správce front do úložiště MSCS” na stránce 480
- “Vložení správce front pod řízení MSCS” na stránce 482

Sdělování MSCS, kteří správci front mají být spravováni

Můžete zvolit, kteří správci front jsou umístěni pod řízení MSCS, a to pomocí nástroje MSCS Cluster Administrator k vytvoření instance prostředku pro každého takového správce front. Tento proces vám zobrazí seznam prostředků, ze kterého můžete vybrat správce front, kterého má daná instance spravovat.

Soubory protokolu správce front

Při přesouvání správce front do úložiště MSCS přesunete jeho soubory protokolu a datové soubory na sdílený disk (příklad viz “Přesun správce front do úložiště MSCS” na stránce 480).

Před přesunem je vhodné správce front ukončit čistě a provést úplnou zálohu datových souborů a souborů protokolu.

Více správců front

Podpora produktu IBM MQ MSCS umožňuje spustit v každém počítači více správců front a umístit jednotlivé správce front pod řízení MSCS.

Windows *Vždy používat MSCS ke správě klastrů*

Nepokoušejte se provádět operace spuštění a zastavení přímo na žádném správci front pod kontrolou MSCS, a to buď pomocí řídicích příkazů, nebo pomocí konzoly IBM MQ Explorer. Místo toho použijte administrátora klastru MSCS k převedení správce front do režimu online nebo do režimu offline.

Použití administrátora klastrů MSCS částečně zabraňuje možným zmatkům způsobeným hlášením MSCS, že správce front je offline, když jste jej ve skutečnosti spustili mimo řízení MSCS. Závažnější je, že zastavení správce front bez použití MSCS je zjištěno MSCS jako selhání při zahájení překonání selhání na jiný uzel.

Windows *Práce v aktivním/aktivním režimu v MSCS*

Oba počítače v klastru MSCS mohou spouštět správce front v režimu Aktivní/Aktivní. Nemusíte mít zcela nečinný počítač, který pracuje jako pohotovostní režim (ale můžete, pokud chcete, v aktivním/pasivním režimu).

Pokud plánujete používat oba počítače ke spuštění pracovní zátěže, poskytněte každému z nich dostatečnou kapacitu (procesor, paměť, sekundární úložiště) ke spuštění celé pracovní zátěže klastru na uspokojivé úrovni výkonu.

Poznámka: Pokud používáte MSCS společně s Microsoft Transakčním serverem (COM +), **nemůžete** používat režim Aktivní/Aktivní. Je to proto, že použít IBM MQ s MSCS a COM +:

- Aplikační komponenty, které používají podporu IBM MQ COM +, musí být spuštěny na stejném počítači jako DTC (Distributed Transaction Coordinator), který je součástí modelu COM +.
- Správce front musí být také spuštěn na stejném počítači.
- Koordinátor DTC musí být konfigurován jako prostředek MSCS, a proto může být kdykoli spuštěn pouze na jednom z počítačů v klastru.

Windows *Příkaz PostOnlinea příkaz PreOfflinev MSCS*

Tyto příkazy slouží k integraci podpory produktu IBM MQ MSCS s jinými systémy. Můžete je použít k zadání příkazů IBM MQ , s určitými omezeními.

Tyto příkazy zadejte do pole Parametry pro prostředek typu `IBM MQ MSCS`. Můžete je použít k integraci podpory produktu IBM MQ MSCS s jinými systémy nebo procedurami. Můžete například určit název programu, který odesílá poštovní zprávu, aktivuje pager nebo generuje jinou formu výstrahy, která má být zachycena jiným monitorovacím systémem.

Příkaz PostOnlineje vyvolán, když se prostředek změní z režimu offline na online; příkaz PreOfflineje vyvolán pro změnu z režimu online na offline. Při vyvolání jsou tyto příkazy standardně spuštěny ze systémového adresáře Windows . Protože produkt IBM MQ používá 32bitový proces monitorování prostředků na 64bitových systémech Windows , jedná se spíše o adresář `\Windows\SysWOW64` než o adresář `\Windows\system32` . Další informace naleznete v dokumentaci Microsoft o přesměrování souborů v prostředí Windows x64 . Oba příkazy jsou spuštěny pod uživatelským účtem, který se používá ke spuštění služby MSCS Cluster Service; a jsou vyvolány asynchronně; podpora IBM MQ MSCS nečeká na jejich dokončení, než bude pokračovat. Tím se eliminuje riziko, že by mohly blokovat nebo zpozdit další operace klastru.

Tyto příkazy můžete také použít k zadání příkazů IBM MQ , například k restartování kanálů žadatele. Příkazy jsou však spouštěny v časovém okamžiku, kdy se změní stav správce front, takže nejsou určeny k provádění přerušitelných funkcí, a nesmí vytvářet předpoklady o aktuálním stavu správce front; je docela možné, že ihned po převedení správce front do režimu online zadal administrátor příkaz offline.

Chcete-li spouštět programy závislé na stavu správce front, zvažte vytvoření instancí typu prostředku `MSCS Generic Application` , jejich umístění do stejné skupiny MSCS jako prostředek správce front a jejich závislost na prostředku správce front.

Windows *Použití upřednostňovaných uzlů v MSCS*

To může být užitečné při použití režimu Aktivní/Aktivní v MSCS ke konfiguraci *upřednostňovaného uzlu* pro každého správce front. Obecně je však lepší nenastavovat upřednostňovaný uzel, ale spoléhat se na ruční odvolání při selhání.

Na rozdíl od jiných relativně nestavových prostředků může správci front chvíli trvat, než dojde k překonání selhání (nebo zpět) z jednoho uzlu na druhý. Chcete-li se vyvarovat zbytečných výpadků, otestujte obnovený uzel před tím, než se k němu vrátí správce front. To vylučuje použití nastavení odvolání při selhání `immediate` . Můžete nakonfigurovat návrat po selhání tak, aby se vyskytoval mezi určitými časovými obdobími.

Nejbezpečnější cestou je pravděpodobně ruční přesun správce front zpět do požadovaného uzlu, pokud jste si jisti, že je uzel plně obnoven. To vylučuje použití volby `preferred node` .

Windows *Chyby COM + při instalaci na MSCS*

Při instalaci produktu IBM MQ do nově nainstalovaného klastru MSCS může dojít k chybě se Zdrojem COM + a ID události 4691 ohlášeným v protokolu událostí aplikace.

To znamená, že se pokoušíte spustit produkt IBM MQ v prostředí serveru Microsoft Cluster Server (MSCS), když nebyl produkt Microsoft Distributed Transaction Coordinator (MSDTC) nakonfigurován pro spuštění v takovém prostředí. Informace o konfiguraci produktu MSDTC v klastrovaném prostředí naleznete v dokumentaci k produktu Microsoft .

Windows *Podpora obslužných programů MSCS*

Seznam obslužných programů IBM MQ support for Microsoft Cluster Service (MSCS), které lze spustit na příkazovém řádku.

Poznámka: V produktu Windows Server 2016je nový název pro produkt Microsoft Cluster Service (MSCS) Windows Server Failover Clustering (WSFC).

Podpora produktu IBM MQ pro MSCS zahrnuje následující obslužné programy:

Registrovat/zrušit registraci typu prostředku
`haregtyp.exe`

Po *zrušení registrace* typu prostředku IBM MQ MSCS již nelze vytvářet žádné prostředky tohoto typu. MSCS vám neumožňuje zrušit registraci typu prostředku, pokud máte v klastru stále instance tohoto typu:

1. Pomocí administrátora klastru MSCS zastavte všechny správce front, kteří jsou spuštěni pod řízením MSCS, tím, že je převedete do režimu offline, jak je popsáno v tématu “Převedení správce front z MSCS do režimu offline” na stránce 489.
2. Pomocí administrátora klastru MSCS odstraňte instance prostředků.
3. Na příkazovém řádku zrušte registraci typu prostředku zadáním následujícího příkazu:

```
haregtyp /u
```

Chcete-li *registrovat* typ (nebo jej znovu registrovat později), zadejte na příkazový řádek následující příkaz:

```
haregtyp /r
```

Po úspěšné registraci knihoven MSCS musíte restartovat systém, pokud jste tak neučinili od instalace produktu IBM MQ.

Přesunout správce front do úložiště MSCS
`hamvmqm.exe`

Viz “Přesun správce front do úložiště MSCS” na stránce 480.

Odstranit správce front z uzlu
`hadltmqm.exe`

Zvažte případ, kdy jste měli ve svém klastru správce front, který byl přesunut z jednoho uzlu do jiného a nyní jej chcete zničit. Pomocí Průzkumníku IBM MQ jej můžete odstranit na uzlu, na kterém se právě nachází. Položky registru pro tento počítač stále existují na jiném počítači. Chcete-li je odstranit, zadejte na příkazovém řádku v daném počítači následující příkaz:

```
hadltmqm /m qmname
```

kde `qmname` je název správce front, který má být odebrán.

Zkontrolovat a uložit podrobnosti nastavení
`amqmsysn.exe`

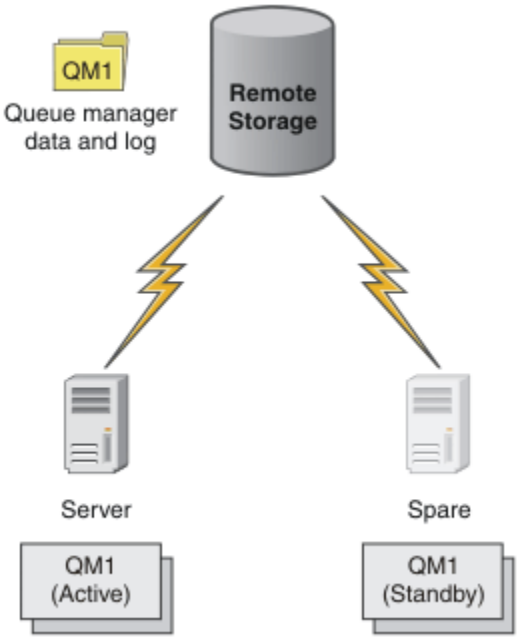
Tento obslužný program zobrazí dialogové okno se všemi podrobnostmi o nastavení podpory produktu IBM MQ MSCS, které mohou být požadovány, pokud zavoláte podporu systému IBM . Existuje volba pro uložení podrobností do souboru.

Multi 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 rezervní instance. Pokud se aktivní instance nezdaří, správce front pro více instancí se automaticky restartuje na záložním serveru.

Příklad konfigurace správce front pro více instancí

Obrázek 72 na stránce 494 zobrazuje příklad konfigurace s více instancemi pro správce front QM1. Produkt IBM MQ je nainstalován na dvou serverech, z nichž jeden je náhradní. Byl vytvořen jeden správce front QM1. Jedna instance QM1 je aktivní a je spuštěna na jednom serveru. Druhá instance QM1 je spuštěna v pohotovostním režimu na druhém serveru, neprovádí aktivní zpracování, ale je připravena převzít od aktivní instance QM1, pokud aktivní instance selže. (V konfiguraci s více instancemi může existovat pouze jedna aktivní instance a jedna rezervní instance správce front.)



Obrázek 72. Správce front s více instancemi

Pokud hodláte používat správce front jako správce front s více instancemi, vytvořte jednoho správce front na jednom ze serverů pomocí příkazu **crtmqm** a umístěte jeho data správce front a protokoly do sdíleného síťového úložiště. Na druhém serveru namísto opětovného vytvoření správce front použijte příkaz **addmqinf** k vytvoření odkazu na data správce front a protokoly v síťovém úložišti.

Nyní můžete spustit správce front z jednoho ze serverů. Každý ze serverů odkazuje na stejná data a protokoly správce front; existuje pouze jeden správce front, který je v daném okamžiku 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, která zpracovává požadavky. Rozdíl spočívá v tom, že při spuštění jako správce front s více instancemi je server, na kterém není spuštěna aktivní instance správce front, spuštěn jako záložní instance, která je připravena převzít od aktivní instance automaticky v případě, že dojde k selhání aktivního serveru.

Jediným ovládacím prvkem, přes který se instance stane aktivní, je pořadí, ve kterém spustíte správce front na obou serverech. První instance, která získá zámky čtení/zápisu do dat správce front, se stane aktivní instancí.

Aktivní instanci můžete po spuštění přehodit na jiný server tak, že zastavíte aktivní instanci pomocí volby přepnutí pro přenos řízení do pohotovostního režimu.

Aktivní instance QM1 má při spuštění výlučný přístup ke sdíleným datům správce front a složkám protokolů. Rezervní instance QM1 zjistí, že aktivní instance selhala, a stane se aktivní instancí. Přebírá data a protokoly QM1 ve stavu, ve kterém byla ponechána aktivní instancí, a přijímá opětovná připojení od klientů a kanálů.

Aktivní instance může selhat z různých příčin, které vedou k převzetí pohotovostního režimu:

- Selhání serveru, který je hostitelem aktivní instance správce front.
- Došlo k selhání konektivity mezi serverem, který je hostitelem aktivní instance správce front, a systémem souborů.
- Funkce Unresponsiveness procesů správce front, zjištěná produktem IBM MQ, která poté vypne správce front.

Informace o konfiguraci správce front můžete přidat na více serverů a zvolit libovolné dva servery, které mají být spuštěny jako dvojice aktivní/záložní. Je zde limit celkem dvou instancí. Nemůžete mít dvě rezervní instance a jednu aktivní instanci.

Další komponenty potřebné k sestavení řešení vysoké dostupnosti

Správce front pro více instancí je součástí řešení vysoké dostupnosti. K vytvoření užitečného řešení vysoké dostupnosti potřebujete další komponenty.

- Opětovné připojení klienta a kanálu pro přenos připojení produktu IBM MQ do počítače, 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: Než budete moci provést údržbu jednotky NFS , musíte zastavit všechny instance správce front s více instancemi, které jsou spuštěny ve vašem prostředí. V případě selhání systému NFS se ujistěte, že máte k dispozici zálohy konfigurace správce front, které je třeba obnovit.
- Odolné sítě a napájecí zdroje, které eliminují jednotlivá místa selhání základní infrastruktury.
- Aplikace, které tolerují překonání selhání. Zejména je třeba věnovat velkou pozornost chování transakčních aplikací a aplikací, které procházejí frontami IBM MQ .
- Monitorování a správa aktivních a rezervních instancí, abyste se ujistili, že jsou spuštěny, a abyste restartovali aktivní instance, které selhaly. Ačkoli se správci front s více instancemi automaticky restartují, je třeba se ujistit, že jsou instance v pohotovostním režimu spuštěny, připraveny k převzetí a že nezdařené instance jsou znovu uvedeny do režimu online jako nové instance v pohotovostním režimu.

Produkt IBM MQ MQI clients a kanály se po aktivaci automaticky znovu připojí ke správci front v pohotovostním režimu. Další informace o opětovném připojení a dalších komponentách v řešení vysoké dostupnosti naleznete v souvisejících tématech. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

podporované platformy

Správce front s více instancemi můžete vytvořit na libovolné jiné platformě nežz/OS .

Pro klienty MQI je podporováno automatické opětovné připojení klienta.

Vytvořit správce front pro více instancí

Vytvořte správce front s více instancemi, vytvořte jej na jednom serveru a nakonfigurujte produkt IBM MQ na jiném serveru. Správci front s více instancemi sdílejí data a protokoly správce front.

Většina úsilí při vytváření správce front s více instancemi je úlohou nastavení sdílených dat a souborů protokolu správce front. Musíte vytvořit sdílené adresáře v síťovém úložišti a zpřístupnit je ostatním serverům pomocí síťových sdílení. Tyto úlohy musí provádět někdo s administrativním oprávněním, například *root* na systémech AIX and Linux . Kroky jsou následující:

1. Vytvořte sdílení pro datové soubory 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. Spuštěním příkazu **addmqinf** s zkopírovanými daty vytvořte konfiguraci správce front na druhém serveru.

Spuštěním příkazu **crtmqm** znovu nevytvoříte správce front na druhém serveru.

Řízení přístupu k souborům

Musíte dbát na to, aby měl uživatel a skupina `mqm` na všech ostatních serverech oprávnění k přístupu ke sdílením.

V systému AIX and Linuxmusíte na všech systémech nastavit `uid` a `gid` `mqm` jako stejné. Možná budete muset upravit `/etc/passwd` na každém systému, abyste nastavili společné `uid` a `gid` pro `mqm`, a pak znovu zavést systém.

V systému Microsoft Windowsmusí mít ID uživatele, který spouští procesy správce front, úplná oprávnění k řízení adresářů obsahujících data správce front a soubory protokolu. Oprávnění můžete konfigurovat dvěma způsoby:

1. Vytvořte správce front s globální skupinou jako alternativním činitelem zabezpečení. Autorizujte globální skupinu, aby měla úplný řídicí přístup k adresářům obsahujícím data správce front a soubory protokolu; viz “Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows” na stránce 523. Učiňte jméno uživatele, který spouští správce front, členem globální skupiny. Lokálního uživatele nelze nastavit 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 pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498demonstruje, jak nastavit správce front pro více instancí pomocí takto zabezpečených souborů.
2. Vytvořte správce front na řadiči domény tak, aby lokální skupina `mqm` měla rozsah domény "domain local". Zabezpečte sdílení souboru s lokálním doménovým produktem `mqm`a spusťte procesy správce front ve všech instancích správce front ve stejné doménové lokální skupině `mqm` . Úloha “Vytvoření správce front pro více instancí v řadičích domény Windows” na stránce 513demonstruje, jak nastavit správce front pro více instancí pomocí takto zabezpečených souborů.

Informace o konfiguraci

Konfigurujte libovolný počet instancí správce front úpravou informací o konfiguraci správce front IBM MQ pro jednotlivé servery. Každý server musí mít stejnou verzi produktu IBM MQ nainstalovanou na kompatibilní úrovni opravy. Příkazy **dspmqinf** a **addmqinf** vám pomáhají konfigurovat další instance správce front. Případně můžete upravit soubory `mqs.ini` a `qm.ini` přímo. Témata “Vytvoření správce front pro více instancí v systému Linux” na stránce 535, “Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498a “Vytvoření správce front pro více instancí v řadičích domény Windows” na stránce 513 jsou příklady konfigurace správce front pro více instancí.

Na systémech AIX, Linux, and Windows můžete sdílet jeden soubor `mqs.ini` tak, že jej umístíte do sdílení sítě a nastavíte proměnnou prostředí **AMQ_MQS_INI_LOCATION** tak, aby na něj ukazovala.

Omezení

1. Konfigurujte více instancí stejného správce front pouze na serverech se stejným operačním systémem, architekturou a endianness. Například oba počítače musí být buď 32bitové, nebo 64bitové.
2. Všechny instalace produktu IBM MQ musí být na úrovni vydání 7.0.1 nebo vyšší.
3. Aktivní a pohotovostní instalace jsou obvykle udržovány na stejné úrovni údržby. V pokynech pro údržbu jednotlivých upgradů zkontrolujte, zda je nutné provést upgrade všech instalací společně.

   Mějte na paměti, že úrovně údržby pro aktivní a pasivní správce front musí být identické.
4. Data a protokoly správce front lze sdílet pouze mezi správci front, kteří jsou konfigurováni se stejným uživatelem, skupinou a mechanizmem řízení přístupu produktu IBM MQ . IBM i Například síťové sdílení nastavené na serveru Linux může obsahovat oddělená data správce front a protokoly pro správce front AIX and Linux , ale nemůže obsahovat data správce front používaná produktem IBM i.

   IBM i Můžete vytvořit více sdílení na stejném síťovém úložišti pro systémy IBM i a AIX and Linux , pokud jsou sdílení odlišná. Můžete dát různé akcie různých vlastníků. Omezení je důsledkem různých názvů používaných pro uživatele a skupiny IBM MQ mezi AIX and Linuxa IBM i. Skutečnost, že uživatel a skupina mohou mít stejné `uid` a `gid` , omezení neuvolní.
5. Na systémech AIX and Linux nakonfigurujte sdílený systém souborů na síťovém úložišti s `pevným`, přerušitelným, spíše než `měkkým` připojením. Pevné přerušitelné připojení vynutí pozastavení správce front, dokud nebude přerušen systémovým voláním. Měkká připojení nezaručují konzistenci dat po selhání serveru.

6. Sdílené adresáře protokolů a dat nemohou být uloženy v systému souborů FAT nebo NFSv3 . V případě správců front s více instancemi v systému Windowsmusí k síťovému úložišti přistupovat protokol CIFS (Common Internet File System) používaný sítěmi Windows .
7. z/OS Produkt z/OS nepodporuje správce front s více instancemi. Použít skupiny sdílení front.

   Klienti s možností opětovného připojení pracují se správci front z/OS .

Windows *Domény Windows a správci front s více instancemi*

Správce front pro více instancí v systému Windows vyžaduje sdílení dat a protokolů. Sdílení musí být přístupné pro všechny instance správce front spuštěné na různých serverech nebo pracovních stanicích. Konfigurujte správce front a sdílejte je jako součást domény Windows . Správce front může být spuštěn na pracovní stanici nebo serveru domény nebo na řadiči domény.

Důležité: Standardně jsou počítače začínající na Windows 10 verze 1607 a Windows Server 2016 více omezující než dřívější verze produktu Windows.

Tato změna omezuje klienty, kteří mají povoleno provádět vzdálená volání do správce SAM (Security Accounts Manager), a může mít dopad na produkt IBM MQ , když se správci front nedaří spustit. Přístup k SAM je kritický pro fungování produktu IBM MQ , když je IBM MQ nakonfigurován jako doménový účet.

Před konfigurací správce front s více instancemi si přečtěte téma “Zabezpečte nesdílená data a adresáře a soubory protokolů správce front v systému Windows” na stránce 526 a “Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows” na stránce 523 , kde můžete zkontrolovat, jak řídit přístup k datům a souborům protokolu správce front. Témata jsou vzdělávací; chcete-li přejít přímo na nastavení sdílených adresářů pro správce front s více instancemi v doméně Windows ; viz “Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498.

Spustit správce front pro více instancí na pracovních stanicích nebo serverech domény

V produktu IBM WebSphere MQ 7.1jsou správci front s více instancemi spouštěny na pracovní stanici nebo serveru, který je členem domény. Chcete-li spustit správce front s více instancemi v systému Windows, potřebujete řadič domény, souborový server a dvě pracovní stanice nebo servery, na kterých je spuštěn stejný správce front připojený ke stejné doméně.

Změna, která umožňuje spustit správce front s více instancemi na libovolném serveru nebo pracovní stanici v doméně, spočívá v tom, že nyní můžete vytvořit správce front s další skupinou zabezpečení. Další skupina zabezpečení je předána v příkazu **crtmqm** v parametru -a . Zabezpečte adresáře, které obsahují data a protokoly správce front, pomocí skupiny. 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. Poskytnutím rozsahu domény skupiny i ID uživatele má 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 a také členem lokální skupiny mqm .

Podrobnosti o vytvoření správce front pro více instancí naleznete v části “Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498 .

Pro konfiguraci domény a doménových serverů a pracovních stanic je vyžadováno více kroků. Musíte 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 jejich protokolům a datovým souborům, přečtěte si téma “Zabezpečte nesdílená data a adresáře a soubory protokolů správce front v systému Windows” na stránce 526. Téma obsahuje dvě úlohy, které vám pomohou porozumět požadovaným krokům. Jedná se o úlohy “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 528 a “Čtení a zápis dat a souborů protokolu autorizovaných alternativní lokální skupinou zabezpečení” na stránce 531. Další téma, “Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows” na stránce 523, vysvětluje, jak zabezpečit sdílené adresáře obsahující data správce front a soubory protokolu pomocí alternativní skupiny zabezpečení.

Téma obsahuje čtyři úlohy pro nastavení domény Windows , vytvoření sdílené složky, instalaci produktu IBM MQ for Windowsa konfiguraci správce front pro použití sdílené složky. Úlohy jsou následující:

1. “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 501.
2. “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 505.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows” na stránce 507.
4. “Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení” na stránce 510.

Poté můžete provést úlohu “Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498pomocí domény. Proveďte tyto úlohy, abyste prozkoumali nastavení správce front pro více instancí před přenosem vašich znalostí do produkční domény.

Spustit správce front s více instancemi na řadičích domény

Data správce front lze zabezpečit pomocí skupiny `mqm` domény. Jak vysvětluje téma “Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows” na stránce 523 , nemůžete sdílet adresáře zabezpečené lokální skupinou `mqm` na pracovních stanicích nebo serverech. Avšak na řadičích domény mají všechny skupiny a činitelé rozsah domény. Pokud nainstalujete produkt IBM MQ for Windows na řadič domény, data a soubory protokolu správce front budou zabezpečeny pomocí skupiny domény `mqm` , kterou lze sdílet. Chcete-li konfigurovat správce front pro více instancí v řadičích domény, postupujte podle pokynů v úloze “Vytvoření správce front pro více instancí v řadičích domény Windows” na stránce 513 .

Související informace

Správa autorizace a řízení přístupu

Jak používat uzly klastru serveru Windows jako řadiče domény

Windows *Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows*

Příklad ukazuje, jak nastavit správce front pro více instancí v systému Windows na pracovní stanici nebo serveru, který je součástí domény systému Windows . Server nemusí být řadičem domény. Nastavení demonstruje související koncepty, spíše než produkční měřítko. Příklad je založen na serveru Windows Server 2008. Tyto kroky se mohou lišit v jiných verzích serveru Windows .

V konfiguraci produkčního měřítka možná budete muset upravit konfiguraci na existující doménu. Můžete například definovat různé skupiny domén pro autorizaci různých sdílení a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
: Řadič domény serveru Windows Server 2008. Vlastní doménu *`wmq.example.com`* , která obsahuje *`Sun`*, *`mars`*a *`venus`*. Pro účely ilustrace se používá také jako souborový server.

mars
: Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *`QMGR`*.

venus
: Windows Server 2008 použitý jako druhý server IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *`QMGR`*.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

V systému Windowsnení nutné ověřovat systém souborů, v němž plánujete ukládat data správce front a soubory protokolu. Kontrolní proceduru Ověření chování sdíleného systému souborůlze použít pro AIX and Linux. V systému Windowsjsou kontroly vždy úspěšné.

Proveďte kroky v následujících úlohách. Úlohy vytvoří řadič domény a doménu, nainstalují produkt IBM MQ for Windows na jeden server a vytvoří sdílení souborů pro data a soubory protokolu. Pokud konfigurujete existující řadič domény, může být užitečné vyzkoušet kroky na novém serveru Windows Server 2008. Kroky můžete přizpůsobit své doméně.

1. “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 501.
2. “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 505.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows” na stránce 507.
4. “Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení” na stránce 510.

Informace o této úloze

Tato úloha je jednou z posloupností úloh konfigurace řadiče domény a dvou serverů v doméně pro spouštění instancí správce front. V této úloze nakonfigurujete druhý server, *venus*, ke spuštění jiné instance správce front *QMGR*. Postupujte podle kroků v této úloze a vytvořte druhou instanci správce front *QMGR*a otestujte, zda funguje.

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 správce front s jednou nebo více instancemi.

Postup

1. Nakonfigurujte druhý server pro spuštění IBM MQ for Windows.
   a) Chcete-li vytvořit druhý server domény, postupujte podle kroků v úloze “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 505 . V této posloupnosti úloh se druhý server nazývá *venus*.

      Tip: Vytvořte druhou instalaci s použitím stejných předvoleb instalace pro produkt IBM MQ na každém ze dvou serverů. Pokud se výchozí nastavení liší, možná budete muset upravit proměnné Předpona a InstallationName v sekci *QMGR* **QueueManager** v IBM MQ konfiguračním souboru mqs.ini. Proměnné odkazují na cesty, které se mohou lišit pro jednotlivé instalace a správce front na jednotlivých serverech. Pokud cesty zůstanou na všech serverech stejné, je jednodušší konfigurovat správce front pro více instancí.
2. Vytvořte druhou instanci *QMGR* na *venus*.
   a) Pokud *QMGR* na *mars* neexistuje, proveďte úlohu “Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení” na stránce 510, abyste ji vytvořili.
   b) Zkontrolujte, zda jsou hodnoty parametrů Předpona a InstallationName správné pro *venus*.

      V systému *mars*spusťte příkaz **dspmqinf** :

      ```
      dspmqinf QMGR
      ```

      Odezva systému:

      ```
      QueueManager:
      Name=QMGR
      Directory=QMGR
      Prefix=C:\ProgramData\IBM\MQ
      ```

```
DataPath=\\sun\wmq\data\QMGR
InstallationName=Installation1
```

c) Zkopírujte strojově čitelnou formu sekce **QueueManager** do schránky.

V systému *mars* spusťte příkaz **dspmqinf** znovu s parametrem `-o příkaz` .

```
dspmqinf -o command QMGR
```

Odezva systému:

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

d) V systému *venus* spusťte příkaz **addmqinf** ze schránky a vytvořte instanci správce front v systému *venus*.

V případě potřeby upravte příkaz tak, aby byly v parametrech `Předpona` nebo `InstallationName` rozdíly.

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

```
IBM MQ configuration information added.
```

3. Spusťte správce front *QMGR* v systému *venus*, což povolí instance v pohotovostním režimu.

a) Kontrola *QMGR* zapnuto *mars* je zastavena.

V systému *mars*spusťte příkaz **dspmq** :

```
dspmq -m QMGR
```

Odezva systému závisí na způsobu zastavení správce front. Příklad:

```
C:\Users\Administrator>dspmq -m QMGR
QMNAME(QMGR) STATUS(Ended immediately)
```

b) V systému *venus* spusťte příkaz **strmqm** , který spustí *QMGR* povolující rezervní databáze:

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

Výsledky

Chcete-li otestovat přepnutí správce front s více instancemi, postupujte takto:

1. V systému *mars*spusťte příkaz **strmqm** , který spustí *QMGR* povolující rezervní databáze:

   ```
   strmqm -x QMGR
   ```

   Odezva systému:

   ```
   IBM MQ queue manager 'QMGR' starting.
   The queue manager is associated with installation 'Installation1'.
   A standby instance of queue manager 'QMGR' has been started.
   The active instance is running elsewhere.
   ```

2. V systému *venus* spusťte příkaz **endmqm** :

   ```
   endmqm -r -s -i QMGR
   ```

   Odezva systému na *venus*:

   ```
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ending.
   IBM MQ queue manager 'QMGR' ended, permitting switchover to
   a standby instance.
   ```

   A na *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

Ověření správce front s více instancemi pomocí ukázkových programů; viz “Ověření správce front pro více instancí v systému Windows” na stránce 521.

Windows *Vytvoření Active Directory a domény DNS v systému Windows*

Tato úloha vytvoří doménu *wmq.example.com* na řadiči domény Windows 2008 s názvem *sun*. Konfiguruje globální skupinu Domain mqm v doméně se správnými právy a s jedním uživatelem.

V konfiguraci produkčního měřítka možná budete muset upravit konfiguraci na existující doménu. Můžete například definovat různé skupiny domén pro autorizaci různých sdílení a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
: Řadič domény serveru Windows Server 2008. Vlastní doménu *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
: Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Windows Server 2008 použitý jako druhý server IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *QMGR*.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

1. Kroky úlohy jsou konzistentní s produktem Windows Server 2008, který je nainstalován, ale není nakonfigurován s žádnými rolemi. Pokud konfigurujete existující řadič domény, může být užitečné vyzkoušet kroky na novém serveru Windows Server 2008. Kroky můžete přizpůsobit své doméně.

Informace o této úloze

V této úloze vytvoříte Active Directory a doménu DNS na novém řadiči domény. Poté jej nakonfigurujete tak, aby byl připraven k instalaci produktu IBM MQ na jiných serverech a pracovních stanicích, které se připojují k doméně. Pokud nejste obeznámeni s instalací a konfigurací služby Active Directory pro vytvoření domény Windows , postupujte podle této úlohy. Chcete-li vytvořit konfiguraci správce front pro více instancí, musíte vytvořit doménu Windows . Úloha není určena k tomu, aby vás vedla nejlepším způsobem, jak nakonfigurovat doménu Windows . Chcete-li implementovat správce front s více instancemi v produkčním prostředí, musíte nahlédnout do dokumentace k produktu Windows .

Během úlohy provedete následující kroky:

1. Nainstalujte službu Active Directory.
2. Přidejte doménu.
3. Přidejte doménu do DNS.
4. Vytvořte globální skupinu `Domain mqm` a udělte jí správná práva.
5. Přidejte uživatele a učiňte jej členem 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 “Domény Windows a správci front s více instancemi” na stránce 497.

Pro účely úlohy je název hostitele řadiče domény *sun*a dva servery IBM MQ se nazývají *mars* a *venus*. Doména se nazývá *wmq.example.com*. Můžete nahradit všechny názvy kurzívou v úloze názvy dle vlastního výběru.

Postup

1. Přihlaste se k řadiči domény *sun*jako lokální administrátor nebo administrátor produktu `Workgroup` .

   Pokud je server již konfigurován jako řadič domény, musíte se přihlásit jako administrátor domény.
2. Spusťte průvodce Active Directory Domain Services.

   a) Klepněte na tlačítko **Spustit** > **Spustit ...** Zadejte `dcpromo` a klepněte na tlačítko **OK**.

   Pokud již nejsou binární soubory Active Directory nainstalovány, produkt Windows tyto soubory nainstaluje automaticky.
3. V prvním okně průvodce ponechte zaškrtávací políčko **Použít rozšířený režim instalace** nezaškrtnuté. Klepněte na tlačítko **Další** > **Další** a klepněte na volbu **Vytvořit novou doménu v nové doménové struktuře** > **Další**.
4. Zadejte *wmq.example.com* do pole **FQDN kořenové domény doménové struktury** . Klepněte na tlačítko **Další**.
5. V okně Nastavit úroveň funkčnosti doménové struktury vyberte volbu **Windows Server 2003**nebo novější ze seznamu **Úroveň funkčnosti doménové struktury** > **Další**.

   Nejstarší úroveň serveru Windows , kterou produkt IBM MQ podporuje, 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 úroveň funkčnosti doménové struktury na **Windows Server 2003**.
7. Otevře se okno Další volby řadiče domény, ve kterém je jako další volba vybrána volba **Server DNS** . Klepnutím na tlačítko **Další** a **Ano** vymažte okno s varováním.

   Tip: Pokud je server DNS již nainstalován, tato volba se vám nepředloží. Chcete-li tuto úlohu přesně sledovat, odeberte všechny role z tohoto řadiče domény a začněte znovu.
8. Ponechte adresáře `Database`, `Log Files`a SYSVOL beze změny; klepněte na tlačítko **Další**.
9. Zadejte heslo do polí **Heslo** a **Potvrdit heslo** v okně Heslo administrátora režimu obnovy adresářových služeb. Klepněte na tlačítko **Další** > **Další**. V závěrečném okně průvodce vyberte volbu **Znovu zavést po dokončení** .
10. Když se řadič domény znovu spustí, přihlaste se jako uživatel *wmq*\`Adminstrator`.

    Správce serveru se spustí automaticky.
11. Otevřete složku *wmq.example.com*\`Users` .
    a) Otevřete **Správce serveru** > **Role** > **Active Directory Doménové služby** > ***wmq.example.com*** > **Uživatelé**.
12. Klepněte pravým tlačítkem myši na volbu **Uživatelé** > **Nový** > **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 Prepare IBM MQ Wizard na pracovní stanici nebo serveru domény. Způsobí to, že Prepare IBM MQ Wizard automaticky přidá skupinu `Domain mqm` do lokální skupiny `mqm` v každé nové instalaci produktu IBM MQ v dané doméně.
       - Pracovní stanice nebo servery můžete instalovat i v doméně bez globální skupiny `Domain mqm`. Pokud tak učiníte, musíte definovat skupinu se stejnými vlastnostmi jako skupina `Domain mqm` . Tuto skupinu nebo uživatele, kteří jsou jejími členy, musíte určit jako členy lokální skupiny `mqm`, kdekoli je produkt IBM MQ v nějaké doméně nainstalován. Uživatele domény můžete zahrnout do více skupin. Vytvořte několik skupin domén, kde každá skupina odpovídá sadě instalací, kterou chcete spravovat samostatně. Uživatele domén rozdělte podle instalací, které spravují, do různých skupin domén. Jednotlivé skupiny domén přidejte do lokální skupiny `mqm` v různých instalacích produktu IBM MQ. Pouze uživatelé domény ve skupinách domén, které jsou členy specifické lokální skupiny `mqm`, mohou vytvářet, spravovat a spouštět správce front pro tuto instalaci.
       - Uživatel domény, kterého nominujete při instalaci produktu IBM MQ na pracovní stanici nebo serveru 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 skupinách** a **Povolit Číst groupMembershipSAM** k právům globální skupiny `Domain mqm` .
    a) V řádku s akcemi správce serveru klepněte na volbu **Pohled** > **Rozšířené vlastnosti**.
    b) V navigačním stromu Správce serveru klepněte na položku **Uživatelé** .
    c) V okně Uživatelé klepněte pravým tlačítkem myši na volbu **Domain mqm** > **Vlastnosti**
    d) Klepněte na volbu **Zabezpečení** > **Rozšířené** > **Přidat ...**. Zadejte `Domain mqm` a klepněte na volbu **Zkontrolovat názvy** > **OK**.

       Pole **Název** je předem vyplněno řetězcem `Domain mqm (`*domain name*`\Domain mqm)`.
    e) Klepněte na volbu **Vlastnosti**. V seznamu **Použít na** vyberte položku **Podřízené objekty uživatele**.
    f) Ze seznamu **Oprávnění** vyberte zaškrtávací políčka **Číst členství ve skupinách** a **Číst groupMembershipSAM Povolit** ; klepněte na tlačítko **OK** > **Použít** > **OK** > **OK**.

14. Přidejte dva nebo více uživatelů do globální skupiny `Domain mqm` .

    Jeden uživatel, v příkladu *wmquser1* , spustí službu IBM MQ a druhý uživatel, *wmquser2* , se použije interaktivně.

    Uživatel domény musí vytvořit správce front, který používá alternativní skupinu zabezpečení v konfiguraci domény. Nestačí, aby bylo ID uživatele administrátorem, i když má administrátor oprávnění ke spuštění příkazu **crtmqm** . Uživatel domény, který může být administrátorem, musí být členem lokální skupiny `mqm` i alternativní skupiny zabezpečení.

    V tomto příkladu učiníte členy *wmquser1* a *wmquser2* globální skupiny `Domain mqm` . Prepare IBM MQ Wizard automaticky konfiguruje `Domain mqm` jako člena lokální skupiny `mqm` , kde je spuštěn průvodce.

    Chcete-li spustit službu IBM MQ pro každou instalaci produktu IBM MQ na jednom počítači, musíte zadat jiného uživatele. Stejné uživatele můžete znovu použít na různých počítačích.

    a) V navigačním stromu Správce serveru klepněte na položku **Uživatelé** > **Nový** > **Uživatel**

    b) V okně Nový objekt-Uživatel zadejte do pole **Přihlašovací jméno uživatele** hodnotu *wmquser1* . Zadejte *WebSphere* do pole **Křestní jméno** a *MQ1* do pole **Příjmení** . Klepněte na tlačítko **Další**.

    c) Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a vymažte zaškrtávací políčko **Uživatel musí změnit heslo při příštím přihlášení** . Klepněte na tlačítko **Další** > **Dokončit**.

    d) V okně Uživatelé klepněte pravým tlačítkem myši na položku ***WebSphere MQ*** > **Přidat do skupiny ...**. Zadejte `Domain mqm` a klepněte na tlačítko **Zkontrolovat názvy** > **OK** > **OK**.

    e) Opakujte kroky a až d a přidejte *WebSphere MQ2* jako *wmquser2* .

15. Spuštění produktu IBM MQ jako služby.

    Pokud potřebujete spustit produkt IBM MQ jako službu a poté udělit uživateli domény (který jste získali od administrátora domény) přístup ke spuštění jako služba, postupujte takto:

    a) Klepněte na tlačítko **Spustit > Spustit ...**.

    Zadejte příkaz `secpol.msc` a klepněte na tlačítko **OK**.

    b) Otevřete volbu **Nastavení zabezpečení > Lokální zásady > Přiřazení uživatelských práv**.

    V seznamu zásad klepněte pravým tlačítkem myši na volbu **Přihlásit se jako služba > Vlastnosti**.

    c) Klepněte na volbu **Přidat uživatele nebo skupinu ...**

    Zadejte jméno uživatele, které jste získali od administrátora domény, a klepněte na volbu **Zkontrolovat jména** .

    d) Budete-li vyzváni oknem Zabezpečení Windows , zadejte jméno uživatele a heslo uživatele nebo administrátora účtu s dostatečným oprávněním a klepněte na tlačítko **OK > Použít > OK**.

    Zavřete okno Lokální zásada zabezpečení.

    Poznámka: Na systémech Windows Server 2008 a Windows Server 2012 je řízení uživatelských účtů (UAC) standardně povoleno.

    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 další úlohou “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 505.

Související úlohy

Windows Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows

Windows Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows

Windows Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení

Windows *Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows*

V této úloze nainstalujete a nakonfigurujete produkt IBM MQ na serveru nebo pracovní stanici v doméně *wmq.example.com* Windows .

V konfiguraci produkčního měřítka možná budete muset upravit konfiguraci na existující doménu. Můžete například definovat různé skupiny domén pro autorizaci různých sdílení a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
Řadič domény serveru Windows Server 2008. Vlastní doménu *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Windows Server 2008 použitý jako druhý server IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *QMGR*.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

Důležité: Standardně jsou počítače začínající na Windows 10 verze 1607 a Windows Server 2016 více omezující než dřívější verze produktu Windows.

Tato změna omezuje klienty, kteří mají povoleno provádět vzdálená volání do správce SAM (Security Accounts Manager), a může mít dopad na produkt IBM MQ , když se správci front nedaří spustit. Přístup k SAM je kritický pro fungování produktu IBM MQ , když je IBM MQ nakonfigurován jako doménový účet.

1. Postupujte podle pokynů v části "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 501 a vytvořte řadič domény *sun*pro doménu *wmq.example.com*. Změňte názvy kurzívou tak, aby vyhovovaly vaší konfiguraci.
2. Viz Požadavky na hardware a software na Windows systémech , kde naleznete další verze produktu Windows , na kterých můžete spustit produkt IBM MQ .

Informace o této úloze

V této úloze nakonfigurujete server Windows Server 2008 s názvem *mars*jako člena domény *wmq.example.com* . Nainstalujete produkt IBM MQa nakonfigurujete instalaci tak, aby byla spuštěna 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 "Domény Windows a správci front s více instancemi" na stránce 497.

Pro účely úlohy je název hostitele řadiče domény *sun*a dva servery IBM MQ se nazývají *mars* a *venus*. Doména se nazývá *wmq.example.com*. Můžete nahradit všechny názvy kurzívou v úloze názvy dle vlastního výběru.

Postup

1. Přidejte řadič domény *sun.wmq.example.com* do *mars* jako server DNS.
   a) V systému *mars*se přihlaste jako *mars*\Administrator a klepněte na tlačítko **Spustit**.
   b) Klepněte pravým tlačítkem myši na volbu **Síť** > **Vlastnosti** > **Spravovat síťová připojení**.
   c) Klepněte pravým tlačítkem myši na síťový adaptér, klepněte na volbu **Vlastnosti**.

      Systém odpoví oknem Vlastnosti připojení k místní síti s položkami, které připojení používá.

d) Ze seznamu položek v okně Vlastnosti připojení k místní síti vyberte volbu **Internet Protocol verze 4** nebo **Internet Protocol IBM WebSphere MQ 6** . Klepněte na volbu **Vlastnosti** > **Rozšířené ...** a klepněte na kartu **DNS** .

e) Pod adresami serveru DNS klepněte na tlačítko **Přidat ...**.

f) Zadejte adresu IP řadiče domény, což je také server DNS, a klepněte na tlačítko **Přidat**.

g) Klepněte na volbu **Připojit tyto přípony DNS** > **Přidat ...**.

h) Zadejte *wmq.example.com* a klepněte na tlačítko **Přidat**.

i) Zadejte *wmq.example.com* do pole **Přípona DNS pro toto připojení** .

j) Vyberte volbu **Registrovat adresu tohoto připojení v DNS** a **Použít příponu tohoto připojení v registraci DNS**. Klepněte na tlačítko **OK** > **OK** > **Zavřít**

k) Otevřete příkazové okno a zadejte příkaz **ipconfig /all** , abyste zkontrolovali nastavení TCP/IP.

2. V systému *mars*přidejte počítač do domény *wmq.example.com* .

a) Klepněte na tlačítko **Spustit** .

b) Klepněte pravým tlačítkem myši na volbu **Počítač** > **Vlastnosti**. V oddílu Nastavení názvu počítače, domény a pracovní skupiny klepněte na volbu **Změnit nastavení**.

c) V oknech Vlastnosti systému klepněte na volbu **Změnit ...**.

d) Klepněte na volbu Doména, zadejte *wmq.example.com*a klepněte na tlačítko **OK**.

e) Zadejte **Jméno uživatele** a **Heslo** administrátora řadiče domény, který má oprávnění povolit počítači připojení k doméně, a klepněte na tlačítko **OK**.

f) Klepněte na tlačítko **OK** > **OK** > **Zavřít** > **Restartovat nyní** v reakci na zprávu "Vítejte v *wmq.example.com* doméně" .

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 *mars* správně uveden v okně Počítače.

4. Nainstalujte IBM MQ for Windows na *mars*.

Další informace o spuštění průvodce instalací produktu IBM MQ for Windows naleznete v tématu Instalace IBM MQ serveru na systému Windows .

a) V systému *mars*se přihlaste jako lokální administrátor *mars*\Administrator.

b) Spusťte příkaz **Setup** na instalačním médiu produktu IBM MQ for Windows .

Spustí se aplikace příručního panelu IBM MQ .

c) Klepnutím na volbu **Požadavky na software** zkontrolujte, zda je nainstalován předem vyžadovaný software.

d) Klepněte na volbu **Konfigurace sítě** > **Ano** , chcete-li nakonfigurovat ID uživatele domény.

Úloha “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 501konfiguruje ID uživatele domény pro tuto sadu úloh.

e) Klepněte na volbu **IBM MQ Instalace**, vyberte jazyk instalace a klepněte na volbu Spustit instalační program IBM MQ .

f) Potvrďte licenční smlouvu a klepnutím na tlačítko **Další** > **Další** > **Instalovat** přijměte výchozí konfiguraci. Počkejte na dokončení instalace a klepněte na tlačítko **Dokončit**.

Můžete změnit název instalace, instalovat různé komponenty, konfigurovat jiný adresář pro data a protokoly správce front nebo instalovat do jiného adresáře. Pokud ano, klepněte na volbu **Vlastní** a nikoli na volbu **Typická**.

Produkt IBM MQ je nainstalován a instalační program spustí produkt Prepare IBM MQ Wizard.

Důležité: Průvodce ještě nespouštějte.

5. Nakonfigurujte uživatele, který bude spouštět službu IBM MQ , s právem **Spustit jako službu** .

Zvolte, zda chcete nakonfigurovat lokální skupinu `mqm` , skupinu `Domain mqm` nebo uživatele, který bude spouštět službu IBM MQ s právem. V tomto příkladu dáte uživateli právo.

a) Klepněte na volbu **Spustit** > **Spustit ...**, Zadejte příkaz **`secpol.msc`** a klepněte na tlačítko **OK**.

b) Otevřít **Nastavení zabezpečení** > **Lokální zásady** > **Přiřazení uživatelských práv**. V seznamu zásad klepněte pravým tlačítkem myši na volbu **Přihlásit se jako služba** > **Vlastnosti** .

c) Klepněte na volbu **Přidat uživatele nebo skupinu ...** a zadejte *`wmquser1`* a klepněte na volbu **Zkontrolovat názvy**

d) Zadejte jméno uživatele a heslo administrátora domény *`wmq`*`\Administratora` klepněte na tlačítko **OK** > **Použít** > **OK**. Zavřete okno Lokální zásada zabezpečení.

6. Spusťte příkaz Prepare IBM MQ Wizard.

Další informace viz Konfigurace IBM MQ s Prepare IBM MQ Wizard.

a) Instalační program produktu IBM MQ spustí soubor Prepare IBM MQ Wizard automaticky.

Chcete-li spustit průvodce ručně, vyhledejte zástupce Prepare IBM MQ Wizard ve složce **Spustit** > **Všechny programy** > **IBM MQ** . Vyberte zástupce, který odpovídá instalaci produktu IBM MQ v konfiguraci s více instalačními možnostmi.

b) Klepněte na tlačítko **Další** a ponechte volbu **Ano** , na kterou jste klepli v odpovědi na otázku "Identifikujte, zda v síti existuje Windows 2000 nebo novější řadič domény".

c) Klepněte na tlačítko **Ano** > **Další** v prvním okně Konfigurace IBM MQ for Windows pro uživatele domény Windows .

d) Ve druhém okně Konfigurace IBM MQ for Windows pro uživatele domény systému Windows zadejte do pole **Doména** hodnotu *`wmq`* . Zadejte *`wmquser1`* do pole **Jméno uživatele** a heslo, pokud je nastaveno, do pole **Heslo** . Klepněte na tlačítko **Další**.

Průvodce nakonfiguruje a spustí soubor IBM MQ s příkazem *wmquser1*.

e) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí 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 528, abyste ověřili, že instalace a konfigurace pracují správně.
2. Proveďte úlohu “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows” na stránce 507, abyste nakonfigurovali sdílení souborů pro uložení dat a souborů protokolu správce front s více instancemi.

Související úlohy

Windows Vytvoření Active Directory a domény DNS v systému Windows

Windows Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows

Windows Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení

Související odkazy

Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service

Windows *Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows*

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 produkčního měřítka možná budete muset upravit konfiguraci na existující doménu. Můžete například definovat různé skupiny domén pro autorizaci různých sdílení a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
Řadič domény serveru Windows Server 2008. Vlastní doménu *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Windows Server 2008 použitý jako druhý server IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *QMGR*.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li provést tuto úlohu přesně podle dokumentace, proveďte kroky v úloze "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 501, abyste vytvořili doménu *sun.wmq.example.com* na řadiči domény *sun*. Změňte názvy kurzívou tak, aby vyhovovaly 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 "Domény Windows a správci front s více instancemi" na stránce 497.

V úloze vytvoříte sdílení obsahující adresář dat a protokolů a globální skupinu pro autorizaci přístupu ke sdílení. Předáte název globální skupiny, která autorizuje sdílení, do příkazu **crtmqm** v parametru `-a` . Globální skupina vám poskytuje flexibilitu oddělení uživatelů tohoto sdílení od uživatelů jiných sdílení. Pokud tuto flexibilitu nepotřebujete, autorizujte sdílení se skupinou `Domain mqm` a nevytvářejte 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 Windows doméně *wmq.example.com*. Sdílení má úplná oprávnění k řízení pro globální skupinu *wmqha*. Nahraďte názvy kurzívou v úloze názvy dle vašeho výběru.

Pro účely této úlohy je řadič domény stejný server jako souborový server. V praktických aplikacích rozdělte adresářové a souborové služby mezi různé servery pro výkon a dostupnost.

Musíte nakonfigurovat ID uživatele, pod kterým je spuštěn správce front, aby byl členem dvou skupin. Musí být členem lokální skupiny `mqm` na serveru IBM MQ a globální skupiny *wmqha* .

V této sadě úloh platí, že pokud je správce front spuštěn jako služba, je spuštěn pod ID uživatele *wmquser1*, takže *wmquser1* musí být členem *wmqha*. Pokud je správce front spuštěn interaktivně, je spuštěn pod ID uživatele *wmquser2*, takže *wmquser2* musí být členem *wmqha*. *wmquser1* i *wmquser2* jsou členy globální skupiny `Domain mqm`. `Domain mqm` je členem lokální skupiny `mqm` na serverech *mars* a *venus* IBM MQ . Proto jsou *wmquser1* a *wmquser2* členy lokální skupiny `mqm` na obou serverech IBM MQ .

Postup

1. Přihlaste se k řadiči domény *sun.wmq.example.com* jako administrátor domény.
2. Vytvořte globální skupinu *wmqha*.
   a) Otevřete **Správce serveru** > **Role** > **Active Directory Doménové služby** > ***wmq.example.com*** > **Uživatelé**.
   b) Otevřete složku *wmq.example.com*`\Users` .
   c) Klepněte pravým tlačítkem myši na volbu **Uživatelé** > **Nový** > **Skupina**.

d) Zadejte *wmqha* do pole **Název skupiny** .

e) Ponechte volbu **Globální** , na kterou jste klepli jako **Rozsah skupiny** a volbu **Zabezpečení** , jako **Typ skupiny**. Klepněte na tlačítko **OK**.

3. Přidejte uživatele domény *wmquser1* a *wmquser2* do globální skupiny *wmqha*.

a) V navigačním stromu Správce serveru klepněte na položku **Uživatelé** a klepněte pravým tlačítkem myši na položku ***wmqha*** > **Vlastnosti** v seznamu uživatelů.

b) Klepněte na kartu Členové v okně *wmqha* Vlastnosti.

c) Klepněte na volbu **Přidat ...** ; Zadejte *wmquser1 ; wmquser2* a klepněte na tlačítko **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 úplná oprávnění k řízení adresářů *c: \wmq* a sdílení.

a) V průzkumníku Windows klepněte pravým tlačítkem myši na ***c: \wmq*** > **Vlastnosti**.

b) Klepněte na kartu **Zabezpečení** a klepněte na volbu **Rozšířené** > **Upravit ...**.

c) Vymažte zaškrtávací políčko **Zahrnout zděditelná oprávnění od vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení Windows .

d) Vyberte řádky pro uživatele v seznamu **položek oprávnění** a klepněte na tlačítko **Odebrat**. V seznamu **položek oprávnění**ponechte řádky pro uživatele SYSTEM, Administrators a CREATOR OWNER.

e) Klepněte na tlačítko **Přidat ...**, a zadejte název globální skupiny *wmqha*. Klepněte na tlačítko **Zkontrolovat názvy** > **OK**.

f) V okně Položka oprávnění pro wmq vyberte volbu **Úplné řízení** v seznamu **Oprávnění**.

g) Klepněte na tlačítko **OK** > **Použít** > **OK** > **OK** > **OK**

h) V průzkumníku Windows klepněte pravým tlačítkem myši na ***c: \wmq*** > **Sdílet ...**.

i) Klepněte na volbu **Rozšířené sdílení ...** a zaškrtněte políčko **Sdílet tuto složku** . Název sdílení ponechte jako *wmq*.

j) Klepněte na volbu **Oprávnění** > **Přidat ...**, a zadejte název globální skupiny *wmqha*. Klepněte na tlačítko **Zkontrolovat názvy** > **OK**.

k) V seznamu **Názvy skupin nebo uživatelů**vyberte položku *wmqha* . Zaškrtněte políčko **Úplné řízení** v seznamu **Oprávnění pro *wmqha*** ; klepněte na tlačítko **Použít**.

l) V seznamu **Názvy skupin nebo uživatelů**vyberte položku *Administrators* . Označte zaškrtávací políčko **Úplné řízení** v seznamu **Oprávnění pro *administrátory*** ; Klepněte na tlačítko **Použít** > **OK** > **OK** > **Zavřít**.

Jak pokračovat dále

Zkontrolujte, zda můžete číst a zapisovat soubory do sdílených adresářů ze všech serverů IBM MQ . Zkontrolujte IBM MQ ID uživatele služby *wmquser1* a interaktivní ID uživatele *wmquser2*.

1. Používáte-li vzdálenou plochu, musíte přidat *wmq**wmquser1* a *wmquser2* do lokální skupiny Remote Desktop Users na systému *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 plochy** > **Vlastnosti** > **Přidat ...**. Zadejte *wmquser1 ; wmquser2* a klepněte na volbu **Zkontrolovat názvy**.

d. Zadejte jméno uživatele a heslo administrátora domény *wmq*\Administratora klepněte na tlačítko **OK** > **Použít** > **OK**.

e. Zavřete okno Místní uživatelé a skupiny.

2. Přihlaste se k produktu *mars* jako *wmq**wmquser1*.

a. Otevřete okno Windows Explorer a zadejte *sun**wmq*.

Systém odpoví otevřením *wmq* sdílení na systému *sun.wmq.example.com*a vypíše adresáře dat a protokolů.

b. Zkontrolujte oprávnění produktu *wmquser1* tak, že vytvoříte soubor v podadresáři dat, přidáte nějaký obsah, přečtete jej a pak jej odstraníte.

3. Přihlaste se k *mars* jako *wmq**wmquser2*a zopakujte kontroly.

4. Chcete-li vytvořit správce front pro použití sdílených adresářů dat a protokolů, proveďte další úlohu. Viz "Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení" na stránce 510.

Související úlohy

Windows Vytvoření Active Directory a domény DNS v systému Windows

Windows Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows

Windows Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení

Windows *Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení*

Tato úloha ukazuje, jak použít příznak -a v příkazu **crtmqm** . Příznak -a poskytuje správci front přístup ke svým protokolovým a datovým souborům ve sdílení vzdálených souborů s použitím alternativní skupiny zabezpečení.

V konfiguraci produkčního měřítka možná budete muset upravit konfiguraci na existující doménu. Můžete například definovat různé skupiny domén pro autorizaci různých sdílení a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
Řadič domény serveru Windows Server 2008. Vlastní doménu *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Windows Server 2008 použitý jako druhý server IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *QMGR*.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

Proveďte kroky v následujících úlohách. Úlohy vytvoří řadič domény a doménu, nainstalují produkt IBM MQ for Windows na jeden server a vytvoří sdílení souborů pro data a soubory protokolu. Pokud konfigurujete existující řadič domény, může být užitečné vyzkoušet kroky na novém serveru Windows Server 2008. Kroky můžete přizpůsobit své doméně.

1. "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 501.
2. "Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows" na stránce 505.
3. "Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows" na stránce 507.

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 “Domény Windows a správci front s více instancemi” na stránce 497.

V této úloze vytvoříte správce front, který uloží jeho data a protokoly do vzdáleného adresáře na souborovém serveru. Pro účely tohoto příkladu je souborový server stejný jako řadič domény. Adresář obsahující složky dat a protokolů je sdílen s úplným oprávněním k řízení uděleným globální skupině `wmqha`.

Postup

1. Přihlaste se k serveru domény *mars*jako lokální administrátor *mars*`\Administrator`.
2. Otevřte příkazové okno.
3. Restartujte službu IBM MQ .

   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* zadáním úplného názvu domény globální skupiny *"wmq\wmqha"*.

   Musíte uvést název UNC (Universal Naming Convention) sdílení *\\sun\wmq*a nepoužívat odkaz na mapovanou jednotku.

   Odezva systému:

   ```
   IBM MQ queue manager created.
   Directory '\\sun\wmq\data\QMGR' created.
   The queue manager is associated with installation '1'
   Creating or replacing default objects for queue manager 'QMGR'
   Default objects statistics : 74 created. 0 replaced.
   Completing setup.
   Setup completed.
   ```

Jak pokračovat dále

Otestujte správce front vložením a získáním zprávy do fronty.

1. Spusťte správce front.

   ```
   strmqm QMGR
   ```

   Odezva systému:

   ```
   IBM MQ queue manager 'QMGR' starting.
   The queue manager is associated with installation '1'.
   5 log records accessed on queue manager 'QMGR' during the log
   replay phase.
   Log replay for queue manager 'QMGR' complete.
   Transaction manager state recovered for queue manager 'QMGR'.
   IBM MQ queue manager 'QMGR' started using V7.1.0.0.
   ```

2. Vytvořte testovací frontu.

   ```
   echo define qlocal(QTEST) | runmqsc QMGR
   ```

   Odezva systému:

   ```
   5724-H72 (C) Copyright IBM Corp. 1994, 2024.  ALL RIGHTS RESERVED.
   Starting MQSC for queue manager QMGR.


   1 : define qlocal(QTEST)
   AMQ8006: IBM MQ queue created.
   One MQSC command read.
   No commands have a syntax error.
   All valid MQSC commands were processed.
   ```

3. Vložte testovací zprávu pomocí ukázkového programu **amqsput**.

   ```
   echo 'A test message' | amqsput QTEST QMGR
   ```

   Odezva systému:

   ```
   Sample AMQSPUT0 start
   target queue is QTEST
   Sample AMQSPUT0 end
   ```

4. Získejte testovací zprávu pomocí ukázkového programu **amqsget**.

   ```
   amqsget QTEST QMGR
   ```

   Odezva systému:

   ```
   Sample AMQSGET0 start
   message A test message
   Wait 15 seconds ...
   no more messages
   Sample AMQSGET0 end
   ```

5. Zastavte správce front.

```
endmqm -i QMGR
```

   Odezva systému:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

   Odezva systému:

```
IBM MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

   Tip: Přidejte volbu `/Q` k příkazům, abyste zabránili náznaku příkazu k odstranění každého souboru nebo adresáře.

```
del /F /S C:\wmq\*.*
rmdir /S C:\wmq
```

Související úlohy

Windows Vytvoření Active Directory a domény DNS v systému Windows

Windows Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows

Windows Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows

Windows *Vytvoření správce front pro více instancí v řadičích domény Windows*

Příklad ukazuje, jak nastavit správce front pro více instancí v systému Windows na řadičích domény. Nastavení demonstruje související koncepty, spíše než produkční měřítko. Příklad je založen na serveru Windows Server 2008. Tyto kroky se mohou lišit v jiných verzích serveru Windows .

Konfigurace používá koncept minidomény nebo "domainlet" ; viz Windows 2000, Windows Server 2003 a Windows Uzly klastru serveru 2008 jako řadiče domény. Chcete-li přidat správce front s více instancemi do existující domény, postupujte podle části “Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498.

Příklad konfigurace se skládá ze tří serverů:

sun
: Server Windows Server 2008 použitý 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 řadič domény IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *QMGR*.

mars
: Windows Server 2008 použitý jako souborový server.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

1. V systému Windowsnení nutné ověřovat systém souborů, v němž plánujete ukládat data správce front a soubory protokolu. Kontrolní proceduru Ověření chování sdíleného systému souborůlze použít pro AIX and Linux. V systému Windowsjsou kontroly vždy úspěšné.
2. Chcete-li vytvořit první řadič domény, postupujte podle pokynů v části “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 501 .
3. Postupujte podle pokynů v části “Přidání druhého řadiče domény Windows do vzorové domény” na stránce 517 , chcete-li přidat druhý řadič domény, nainstalujte produkt IBM MQ for Windows na oba řadiče domény a ověřte instalace.
4. Proveďte kroky uvedené v části “Instalace IBM MQ na řadičích domény Windows v ukázkové doméně” na stránce 518 pro instalaci produktu IBM MQ na dva řadiče domény.

Informace o této úloze

Na souborovém serveru ve stejné doméně vytvořte sdílení pro protokoly a datové adresáře správce front. Dále vytvořte první instanci správce front s více instancemi, který používá sdílení souborů na jednom z řadičů domény. Vytvořte druhou instanci na druhém řadiči domény a nakonec ověřte konfiguraci. Sdílení souboru můžete vytvořit na řadiči domény.

V ukázce je *sun* prvním řadičem domény, *earth* druhým a *mars* je souborový server.

Postup

1. Vytvořte adresáře, které mají 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 řídicí přístup k lokální skupině domény mqma ID uživatele, které používáte k vytvoření správce front. V 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 příkladu je server *mars* ve stejné doméně jako řadiče domény.

   a) V průzkumníku Windows klepněte pravým tlačítkem myši na ***c: \wmq*** > **Vlastnosti**.
   b) Klepněte na kartu **Zabezpečení** a klepněte na volbu **Rozšířené** > **Upravit ...**.
   c) Vymažte zaškrtávací políčko **Zahrnout zděditelná oprávnění od vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení Windows .
   d) Vyberte řádky pro uživatele v seznamu **položek oprávnění** a klepněte na tlačítko **Odebrat**. V seznamu **položek oprávnění**ponechte řádky pro uživatele SYSTEM, Administrators a CREATOR OWNER.
   e) Klepněte na tlačítko **Přidat ...**, a zadejte název lokální skupiny domény *mqm*. Klepněte na volbu **Zkontrolovat názvy** .
   f) Jako odpověď na okno Zabezpečení Windows zadejte název a heslo Domain Administrator a klepněte na tlačítko **OK** > **OK**.
   g) V okně Položka oprávnění pro wmq vyberte volbu **Úplné řízení** v seznamu **Oprávnění**.
   h) Klepněte na tlačítko **OK** > **Použít** > **OK** > **OK** > **OK**
   i) Opakujte kroky e až h a přidejte Domain Administrators.
   j) V průzkumníku Windows klepněte pravým tlačítkem myši na ***c: \wmq*** > **Sdílet ...**.
   k) Klepněte na volbu **Rozšířené sdílení ...** a zaškrtněte políčko **Sdílet tuto složku** . Název sdílení ponechte jako *wmq*.

l) Klepněte na volbu **Oprávnění** > **Přidat ...**, a zadejte název lokální skupiny domény *mqm* ; Domain Administrators. Klepněte na volbu **Zkontrolovat názvy**.

m) Jako odpověď na okno Zabezpečení Windows zadejte název a heslo Domain Administrator a klepněte na tlačítko **OK** > **OK**.

3. Vytvořte správce front *QMGR* na prvním řadiči domény *sun*.

```
crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md \\mars\wmq\data -ld \\mars\wmq\logs QMGR
```

Odezva systému:

```
IBM MQ queue manager created.
Directory '\\mars\wmq\data\QMGR' created.
The queue manager is associated with installation 'Installation1'.
Creating or replacing default objects for queue manager 'QMGR'.
Default objects statistics : 74 created. 0 replaced. 0 failed.
Completing setup.
Setup completed.
```

4. Spusťte správce front v systému *sun*, což povolí instanci v pohotovostním režimu.

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

5. Vytvořte druhou instanci *QMGR* na *earth*.

a) Zkontrolujte, zda jsou hodnoty parametrů Předpona a InstallationName správné pro *earth*.

V systému *sun*spusťte příkaz **dspmqinf** :

```
dspmqinf QMGR
```

Odezva systému:

```
QueueManager:
Name=QMGR
Directory=QMGR
Prefix=C:\ProgramData\IBM\MQ
DataPath=\\mars\wmq\data\QMGR
InstallationName=Installation1
```

b) Zkopírujte strojově čitelnou formu sekce **QueueManager** do schránky.

V systému *sun* spusťte příkaz **dspmqinf** znovu s parametrem -o příkaz .

```
dspmqinf -o command QMGR
```

Odezva systému:

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\mars\wmq\data\QMGR
```

c) V systému *earth* spusťte příkaz **addmqinf** ze schránky a vytvořte instanci správce front v systému *earth*.

V případě potřeby upravte příkaz tak, aby byly v parametrech Předpona nebo InstallationName rozdíly.

```
addmqinf -s QueueManager -v Name= QMGR
-v Directory= QMGR -v Prefix="C:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\mars\wmq\data\QMGR
```

```
IBM MQ configuration information added.
```

6. Spusťte rezervní instanci správce front v systému *earth*.

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
A standby instance of queue manager 'QMGR' has been started. The active
instance is running elsewhere.
```

Výsledky

Ověřte, že se správce front přepne z *sun* na *earth*:

1. V systému *sun*spusťte příkaz:

```
endmqm -i -r -s QMGR
```

Odezva systému na *sun*:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended, permitting switchover to
a standby instance.
```

2. V systému *earth* opakovaně zadejte příkaz:

```
dspmq
```

Odezvy systému:

```
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running)
```

Jak pokračovat dále

Ověření správce front s více instancemi pomocí ukázkových programů; viz “Ověření správce front pro více instancí v systému Windows” na stránce 521.

Související úlohy

“Přidání druhého řadiče domény Windows do vzorové domény” na stránce 517

“Instalace IBM MQ na řadičích domény Windows v ukázkové doméně” na stránce 518

Související informace

Uzly klastru Windows 2000, Windows Server 2003 a Windows Server 2008 jako řadiče domény

Windows *Přidání druhého řadiče domény Windows do vzorové domény*

Přidejte druhý řadič domény do domény *wmq.example.com* , abyste vytvořili doménu Windows , ve které se mají spustit správci front s více instancemi na řadičích domény a souborových serverech.

Příklad konfigurace se skládá ze tří serverů:

sun
: Server Windows Server 2008 použitý 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 řadič domény IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *QMGR*.

mars
: Windows Server 2008 použitý jako souborový server.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

1. Postupujte podle pokynů v části “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 501 a vytvořte řadič domény *sun*pro doménu *wmq.example.com*. Změňte názvy kurzívou tak, aby vyhovovaly vaší konfiguraci.
2. Nainstalujte produkt Windows Server 2008 na server ve výchozí pracovní skupině WORKGROUP. V tomto příkladu má server název *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 “Domény Windows a správci front s více instancemi” na stránce 497.

Postup

1. Přidejte řadič domény *sun.wmq.example.com* do *earth* jako server DNS.
   a) V systému *earth*se přihlaste jako *earth*\Administrator a klepněte na tlačítko **Spustit**.
   b) Klepněte pravým tlačítkem myši na volbu **Síť** > **Vlastnosti** > **Spravovat síťová připojení**.
   c) Klepněte pravým tlačítkem myši na síťový adaptér, klepněte na volbu **Vlastnosti**.

      Systém odpoví oknem Vlastnosti připojení k místní síti s položkami, které připojení používá.
   d) Ze seznamu položek v okně Vlastnosti připojení k místní síti vyberte volbu **Internet Protocol verze 4** nebo **Internet Protocol IBM WebSphere MQ 6** . Klepněte na volbu **Vlastnosti** > **Rozšířené ...** a klepněte na kartu **DNS** .

e) Pod adresami serveru DNS klepněte na tlačítko **Přidat ...**.

f) Zadejte adresu IP řadiče domény, což je také server DNS, a klepněte na tlačítko **Přidat**.

g) Klepněte na volbu **Připojit tyto přípony DNS** > **Přidat ...**.

h) Zadejte *wmq.example.com* a klepněte na tlačítko **Přidat**.

i) Zadejte *wmq.example.com* do pole **Přípona DNS pro toto připojení** .

j) Vyberte volbu **Registrovat adresu tohoto připojení v DNS** a **Použít příponu tohoto připojení v registraci DNS**. Klepněte na tlačítko **OK** > **OK** > **Zavřít**

k) Otevřete příkazové okno a zadejte příkaz **ipconfig /all** , abyste zkontrolovali nastavení TCP/IP.

2. Přihlaste se k řadiči domény *sun*jako lokální administrátor nebo administrátor produktu `Workgroup` .

   Pokud je server již konfigurován jako řadič domény, musíte se přihlásit jako administrátor domény.

3. Spusťte průvodce Active Directory Domain Services.

   a) Klepněte na tlačítko **Spustit** > **Spustit ...** Zadejte `dcpromo` a klepněte na tlačítko **OK**.

   Pokud již nejsou binární soubory Active Directory nainstalovány, produkt Windows tyto soubory nainstaluje automaticky.

4. Nakonfigurujte *earth* jako druhý řadič domény v doméně *wmq.example.com* .

   a) V prvním okně průvodce ponechte zaškrtávací políčko **Použít rozšířený režim instalace** nezaškrtnuté. Klepněte na tlačítko **Další** > **Další** a klepněte na volbu **Vytvořit přidání řadiče domény do existující domény** > **Další**.

   b) Zadejte *wmq* do pole **Zadejte název libovolné domény v této doménové struktuře ...** . Klepne se na přepínač **Alternativní pověření** , klepněte na volbu **Nastavit ...**. Zadejte jméno a heslo administrátora domény a klepněte na tlačítko **OK** > **Další** > **Další** > **Další**.

   c) V okně Další volby řadiče domény přijměte vybrané volby **Server DNS** a **Globální katalog** ; klepněte na tlačítko **Další** > **Další**.

   d) V hesle administrátora režimu obnovy adresářových služeb zadejte **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **Další** > **Další**.

   e) Když jste vyzváni, abyste zadali **Síťová pověření**, zadejte heslo administrátora domény. V závěrečném okně průvodce vyberte volbu **Znovu zavést po dokončení** .

   f) Po určité době se může otevřít okno s chybou **DCPromo** týkající se delegování DNS; klepněte na tlačítko **OK**. Server se znovu spustí.

Výsledky

Po opětovném zavedení systému *earth* se přihlaste jako administrátor domény. Zkontrolujte, zda byla doména `wmq.example.com` replikována do adresáře *earth*.

Jak pokračovat dále

Pokračujte v instalaci produktu IBM MQ ; viz “Instalace IBM MQ na řadičích domény Windows v ukázkové doméně” na stránce 518.

Související úlohy

Windows Instalace IBM MQ na řadičích domény Windows v ukázkové doméně

“Vytvoření Active Directory a domény DNS v systému Windows” na stránce 501

Windows *Instalace IBM MQ na řadičích domény Windows v ukázkové doméně*

Instalovat a konfigurovat instalace produktu IBM MQ na obou řadičích domény v doméně *wmq.example.com* .

Příklad konfigurace se skládá ze tří serverů:

sun
Server Windows Server 2008 použitý 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 řadič domény IBM MQ . Obsahuje druhou instanci správce front s více instancemi s názvem *QMGR*.

mars
Windows Server 2008 použitý jako souborový server.

Nahraďte názvy kurzívou v příkladu názvy dle vašeho výběru.

Než začnete

1. Postupujte podle pokynů v části "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 501 a vytvořte řadič domény *sun*pro doménu *wmq.example.com*. Změňte názvy kurzívou tak, aby vyhovovaly vaší konfiguraci.
2. Postupujte podle pokynů v části "Přidání druhého řadiče domény Windows do vzorové domény" na stránce 517 a vytvořte druhý řadič domény *earth*pro doménu *wmq.example.com*. Změňte názvy kurzívou tak, aby vyhovovaly vaší konfiguraci.
3. Viz Požadavky na hardware a software na Windows systémech , kde naleznete další verze produktu Windows , na kterých můžete spustit produkt IBM MQ .

Informace o této úloze

Instalovat a konfigurovat instalace produktu IBM MQ na obou řadičích domény v doméně *wmq.example.com* .

Postup

1. Nainstalujte systém IBM MQ na systémech *sun* a *earth*.

   Další informace viz Instalace serveru IBM MQ na Windows .

   a) V systémech *sun* i *earth*se přihlaste jako administrátor domény *wmq*\Administrator.

   b) Spusťte příkaz **Setup** na instalačním médiu produktu IBM MQ for Windows .

      Spustí se aplikace příručního panelu IBM MQ .

   c) Klepnutím na volbu **Požadavky na software** zkontrolujte, zda je nainstalován předem vyžadovaný software.

   d) Klepněte na volbu **Konfigurace sítě** > **Ne**.

      Pro tuto instalaci můžete konfigurovat buď ID uživatele domény, nebo ne. Vytvořené ID uživatele je ID lokálního uživatele domény.

   e) Klepněte na volbu **IBM MQ Instalace**, vyberte jazyk instalace a klepněte na volbu Spustit instalační program IBM MQ .

   f) Potvrďte licenční smlouvu a klepnutím na tlačítko **Další** > **Další** > **Instalovat** přijměte výchozí konfiguraci. Počkejte na dokončení instalace a klepněte na tlačítko **Dokončit**.

      Chcete-li změnit název instalace, instalovat různé komponenty, konfigurovat jiný adresář pro data a protokoly správce front nebo instalovat do jiného adresáře, klepněte na volbu **Vlastní** a nikoli na volbu **Typická**.

      Produkt IBM MQ je nainstalován a instalační program spustí produkt Prepare IBM MQ Wizard.

   Instalace IBM MQ for Windows konfiguruje lokální skupinu domény mqma skupinu domény Domain mqm. Stává se Domain mqm členem mqm. Následné řadiče domény ve stejné doméně sdílejí skupiny mqm a Domain mqm .

2. V systémech *earth* i *sun*spusťte příkaz Prepare IBM MQ Wizard.

   Další informace viz Konfigurace IBM MQ s Prepare IBM MQ Wizard.

   a) Instalační program produktu IBM MQ spustí Prepare IBM MQ Wizard automaticky.

      Chcete-li spustit průvodce ručně, vyhledejte zástupce Prepare IBM MQ Wizard ve složce **Spustit** > **Všechny programy** > **IBM MQ** . Vyberte zástupce, který odpovídá instalaci produktu IBM MQ v konfiguraci s více instalačními možnostmi.

   b) Klepněte na tlačítko **Další** a ponechte volbu **Ne** , na kterou jste klepli v odpovědi na otázku "Identifikujte, zda v síti existuje Windows 2000 nebo novější řadič domény" .[1].

   c) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí políček podle potřeby a klepněte na tlačítko **Dokončit**.

   Prepare IBM MQ Wizard vytvoří lokálního uživatele domény `MUSR_MQADMIN` na prvním řadiči domény a jiného lokálního uživatele domény `MUSR_MQADMIN1` na druhém řadiči domény. Průvodce vytvoří službu IBM MQ na každém řadiči s `MUSR_MQADMIN` nebo `MUSR_MQADMIN1` jako uživatel, který se přihlásí ke službě.

3. Definujte uživatele, který má oprávnění k vytvoření správce front.

   Uživatel musí mít právo přihlásit se lokálně a být členem lokální skupiny domény `mqm` . Na řadičích domény nemají uživatelé domény právo se přihlásit lokálně, ale administrátoři ano. Standardně nemá žádný uživatel oba tyto atributy. V této úloze přidejte administrátory domény do lokální skupiny `mqm` domény.

   a) Otevřete **Správce serveru** > **Role** > **Active Directory Doménové služby** > ***wmq.example.com*** > **Uživatelé**.

   b) Klepněte pravým tlačítkem myši na volbu **Domain Admins** > **Přidat do skupiny ...** a zadejte `mqm` ; klepněte na tlačítko **Zkontrolovat názvy** > **OK** > **OK**

Výsledky

1. Zkontrolujte, zda Prepare IBM MQ Wizard vytvořil uživatele domény `MUSR_MQADMIN`:

   a. Otevřete **Správce serveru** > **Role** > **Active Directory Doménové služby** > ***wmq.example.com*** > **Uživatelé**.

   b. Klepněte pravým tlačítkem myši na volbu **MUSR_MQADMIN** > **Vlastnosti ...** > **Člen**a uvidíte, že je členem `Domain users` a `mqm`.

2. Zkontrolujte, zda má `MUSR_MQADMIN` právo spouštět jako službu:

   a. Klepněte naKlepněte na volbu **Spustit** > **Spustit ...**, Zadejte příkaz **`secpol.msc`** a klepněte na tlačítko **OK**.

   b. Otevřít **Nastavení zabezpečení** > **Lokální zásady** > **Přiřazení uživatelských práv**. V seznamu zásad klepněte pravým tlačítkem myši na volbu **Přihlásit se jako služba** > **Vlastnosti** a viz `MUSR_MQADMIN` je uvedeno, že má 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 528, abyste ověřili, že instalace a konfigurace pracují správně.
2. Vraťte se k úloze “Vytvoření správce front pro více instancí v řadičích domény Windows” na stránce 513a dokončete úlohu konfigurace správce front pro více instancí na řadičích domény.

Související úlohy

Windows Přidání druhého řadiče domény Windows do vzorové domény

[1] Můžete nakonfigurovat instalaci pro doménu. Vzhledem k tomu, že všichni uživatelé a skupiny na řadiči domény mají rozsah domény, nezáleží na tom. Instalace produktu IBM MQ je jednodušší, jako by nebyl v doméně.

Související odkazy

Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service

Windows *Ověření správce front pro více instancí v systému Windows*

Pomocí ukázkových programů **amqsghac**, **amqsphac** a **amqsmhac** ověřte konfiguraci správce front pro více instancí. V tomto tématu je uveden příklad konfigurace pro ověření konfigurace správce front pro více instancí na serveru Windows Server 2003.

Ukázkové programy s vysokou dostupností používají automatické opětovné připojení klienta. Dojde-li k selhání připojeného správce front, klient se pokusí znovu připojit ke správci front ve stejné skupině správců front. Popis ukázek, Ukázkové programy vysoké dostupnosti, demonstruje opětovné připojení klienta pomocí jednoho správce front instance pro jednoduchost. Stejné ukázky můžete použít se správci front s více instancemi k ověření konfigurace správce front s více instancemi.

Tento příklad používá konfiguraci s více instancemi popsanou v části “Vytvoření správce front pro více instancí v řadičích domény Windows” na stránce 513. Pomocí konfigurace ověřte, že se správce front pro více instancí přepne na instanci v pohotovostním režimu. Zastavte správce front pomocí příkazu **endmqm** a použijte volbu `-s, switchover,`. Klientské programy se znovu připojí k nové instanci správce front a po malé prodlevě budou pokračovat v práci s novou instancí.

Klient je nainstalován v obrazu 400 MB VMware , na kterém běží produkt Windows 7 Service Pack 1. Z bezpečnostních důvodů je připojen na stejné síti pouze hostitele VMware jako servery domény, na kterých je spuštěn správce front pro více instancí. Sdílí složku `/MQHA` , která obsahuje tabulku připojení klienta, aby se zjednodušila konfigurace.

Ověření překonání selhání pomocí IBM MQ Explorer

Před použitím ukázkových aplikací k ověření překonání selhání spusťte IBM MQ Explorer na každém serveru. Přidejte obě instance správce front do každého průzkumníku pomocí průvodce **Přidat vzdáleného správce front > Připojit přímo ke správci front s více instancemi** . Ujistěte se, že jsou spuštěny obě instance, což umožňuje pohotovostní režim. Zavřete okno se spuštěným obrazem VMware s aktivní instancí, virtuálně vypněte server nebo zastavte aktivní instanci, což umožní přepnutí na záložní instanci a opětovné připojení klientů.

Upozornění: Pokud vypnete server, ujistěte se, že to není ten, který hostuje složku `MQHA` !

Poznámka: Volba **Povolit přepnutí na rezervní instanci** nemusí být v dialogovém okně **Zastavit správce front** k dispozici. Tato volba chybí, protože správce front je spuštěn jako správce front s jednou instancí. Musíte ji 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

Zvolit server pro spuštění aktivní instance

Možná jste vybrali jeden ze serverů jako hostitele adresáře `MQHA` nebo systému souborů. Pokud plánujete testovat překonání selhání zavřením okna VMware , na kterém běží aktivní server, ujistěte se, že to není ten, který hostuje `MQHA` !

Na serveru, na kterém je spuštěna aktivní instance správce front.

1. Upravte *ipaddr1* a *ipaddr2* a uložte následující příkazy v adresáři `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: Ponecháte-li parametr **MCAUSER** prázdný, ID uživatele klienta se odešle na server. 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 spuštěn a zda má řízení správce front, a to buď kontrolou výstupu příkazu **runmqsc** .

```
LISTENER(LISTENER.TCP)CONTROL(QMGR)
LISTENER(LISTENER.TCP)STATUS(RUNNING)
```

Nebo pomocí IBM MQ Explorer , že modul listener TCPIP je spuštěn a má `Control = Queue Manager`.

Na straně klienta

1. Namapujte sdílený adresář `C:\MQHA` na serveru na `N:\` na klientovi.
2. Otevřete příkazový řádek s cestou `N:\`. Nastavte proměnnou prostředí `MQCHLLIB` tak, aby ukazovala na tabulku CCDT (Client Channel Definition Table) na serveru:

```
SET MQCHLLIB=N:\data\QM1\@ipcc
```

3. Na příkazovém řádku zadejte příkazy:

```
start amqsghac TARGET QM1
start amqsmhac -s SOURCE -t TARGET -m QM1
start amqsphac SOURCE QM1
```

Poznámka: Pokud máte problémy, spusťte aplikace na příkazovém řádku, aby se kód příčiny vytiskl 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 spuštěným obrazem VMware s aktivní instancí serveru.
   - Pomocí konzoly IBM MQ Explorerzastavte aktivní instanci správce front, abyste umožnili přepnutí na instanci v pohotovostním režimu a instruovali klienty s možností opětovného připojení, aby se znovu připojili.
2. Tři klienti nakonec zjistí, že připojení je přerušeno, a pak se znovu připojí. Pokud v této konfiguraci zavřete okno serveru, trvá obnovení všech tří připojení přibližně sedm minut. Některá připojení jsou před ostatními znovu zavedena.

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
```

Windows *Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows*

Toto téma popisuje, jak můžete zabezpečit sdílené umístění pro data správce front a soubory protokolu pomocí globální alternativní skupiny zabezpečení. Umístění můžete sdílet mezi různými instancemi správce front spuštěného na různých serverech.

Obvykle nenastavujete sdílené umístění pro data správce front a soubory protokolu. Při instalaci produktu IBM MQ for Windowsinstalační program vytvoří domovský adresář podle vaší volby pro všechny správce front, kteří jsou vytvořeni na daném serveru. Zabezpečuje adresáře s lokální skupinou `mqm` a konfiguruje ID uživatele pro službu IBM MQ pro přístup k adresářům.

Při zabezpečení sdílené složky se skupinou zabezpečení musí mít uživatel, kterému je povolen přístup ke složce, pověření skupiny. Předpokládejme, že složka na vzdáleném souborovém serveru je zabezpečena lokální skupinou `mqm` na serveru s názvem *`mars`*. Učiňte uživatele, který spouští správce front, členem lokální skupiny `mqm` v systému *`mars`*. Uživatel má pověření, která se shodují s pověřeními složky na vzdáleném souborovém serveru. Pomocí těchto pověření může správce front přistupovat ke svým datům a souborům protokolů ve složce. Uživatel, který spouští procesy správce front na jiném serveru, je členem jiné lokální skupiny `mqm` , která nemá odpovídající pověření. Když je správce front spuštěn na jiném serveru než *`mars`*, nemůže přistupovat k datům a souborům protokolu, které vytvořil při spuštění v systému *`mars`*. I když uživatele učiníte uživatelem domény, má jiná pověření, protože musí získat pověření z lokální skupiny `mqm` na systému *`mars`*a nemůže to udělat z jiného serveru.

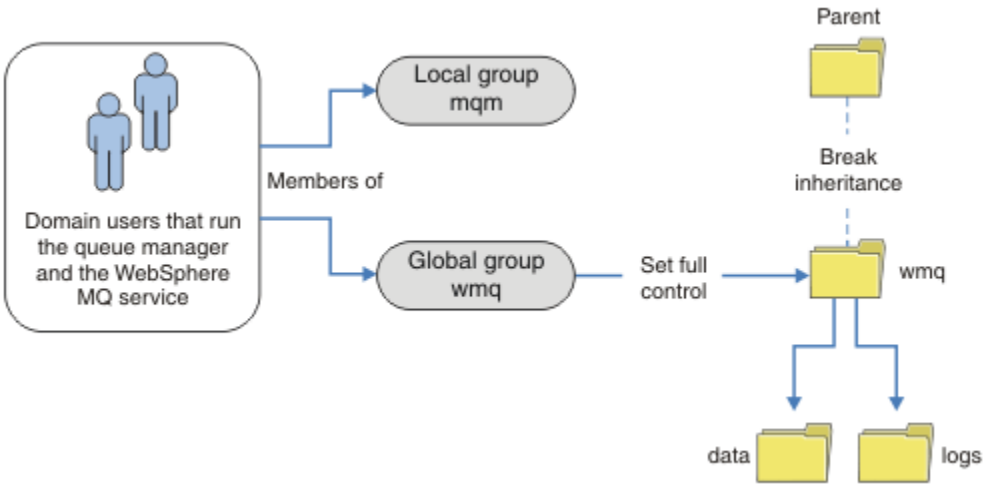
Poskytnutí správce front s globální alternativní skupinou zabezpečení problém vyřeší; viz Obrázek 73 na stránce 524. Zabezpečte vzdálenou složku pomocí globální skupiny. Při vytváření globální skupiny v systému *mars*předejte název globální skupiny správci front. Předejte název globální skupiny jako alternativní skupinu zabezpečení pomocí parametru `-a [ r]` v příkazu **crtmqm** . Pokud přenesete správce front pro spuštění na jiném serveru, bude spolu s ním přenesen název skupiny zabezpečení. Název se přenese v sekci **AccessMode** v souboru `qm.ini` jako `SecurityGroup` ; například:

```
AccessMode:
SecurityGroup=wmq\wmq
```

Sekce **AccessMode** v souboru `qm.ini` také obsahuje `RemoveMQMAccess` ; například:

```
AccessMode:
RemoveMQMAccess=true|false
```

Je-li tento atribut zadán s hodnotou `true`a byla-li zadána také skupina přístupů, není lokální skupině mqm udělen přístup k datovým souborům správce front.

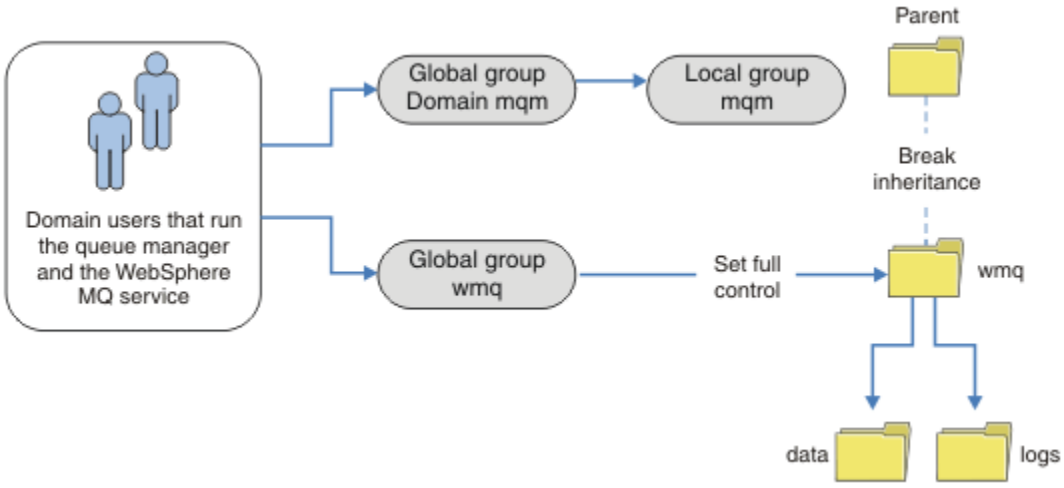


Obrázek 73. Zabezpečení dat a protokolů správce front pomocí alternativní globální skupiny zabezpečení (1)

Pro ID uživatele, se kterým mají procesy správce front pracovat, aby měly odpovídající pověření globální skupiny zabezpečení, musí mít ID uživatele také globální rozsah. Nelze nastavit lokální skupinu nebo činitele jako člena globální skupiny. V produktu Obrázek 73 na stránce 524jsou uživatelé, kteří spouští procesy správce front, zobrazeni jako uživatelé domény.

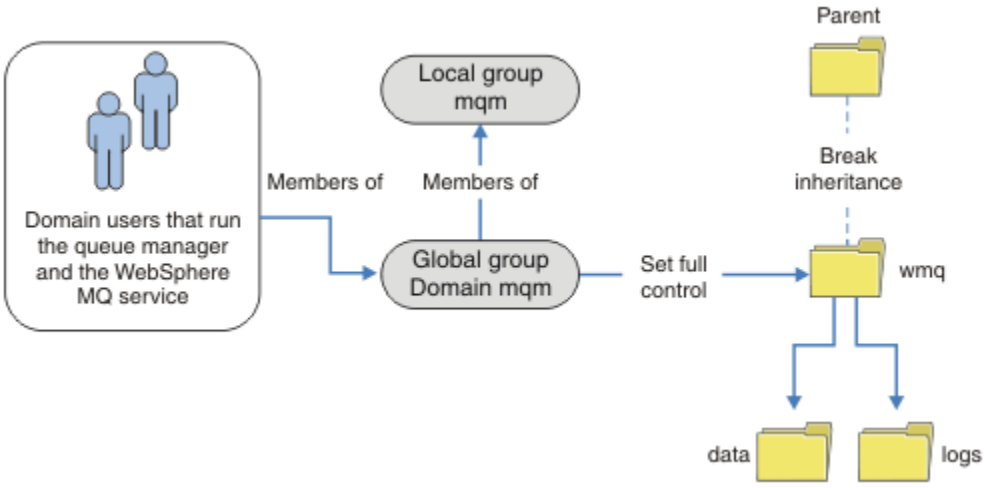
Pokud implementujete mnoho serverů IBM MQ , není seskupení uživatelů v produktu Obrázek 73 na stránce 524 vhodné. Budete muset zopakovat proces přidávání uživatelů do lokálních skupin pro každý server IBM MQ . Místo toho vytvořte globální skupinu `Domain mqm` na řadiči domény a učiňte uživatele, kteří spustí IBM MQ členy skupiny `Domain mqm` ; viz Obrázek 74 na stránce 525. Když instalujete produkt IBM MQ jako instalaci domény, produkt Prepare IBM MQ Wizard automaticky učiní skupinu `Domain mqm` členem lokální skupiny `mqm` . Stejní uživatelé jsou v globálních skupinách `Domain mqm` i `wmq`.

Tip: Stejní uživatelé mohou spustit produkt IBM MQ na různých serverech, ale na individuálním serveru musíte mít různé uživatele, abyste mohli spustit produkt IBM MQ jako službu, a spustit jej interaktivně. Také musíte mít různé uživatele pro každou instalaci na serveru. Obvykle proto `Domain mqm` obsahuje určitý počet uživatelů.



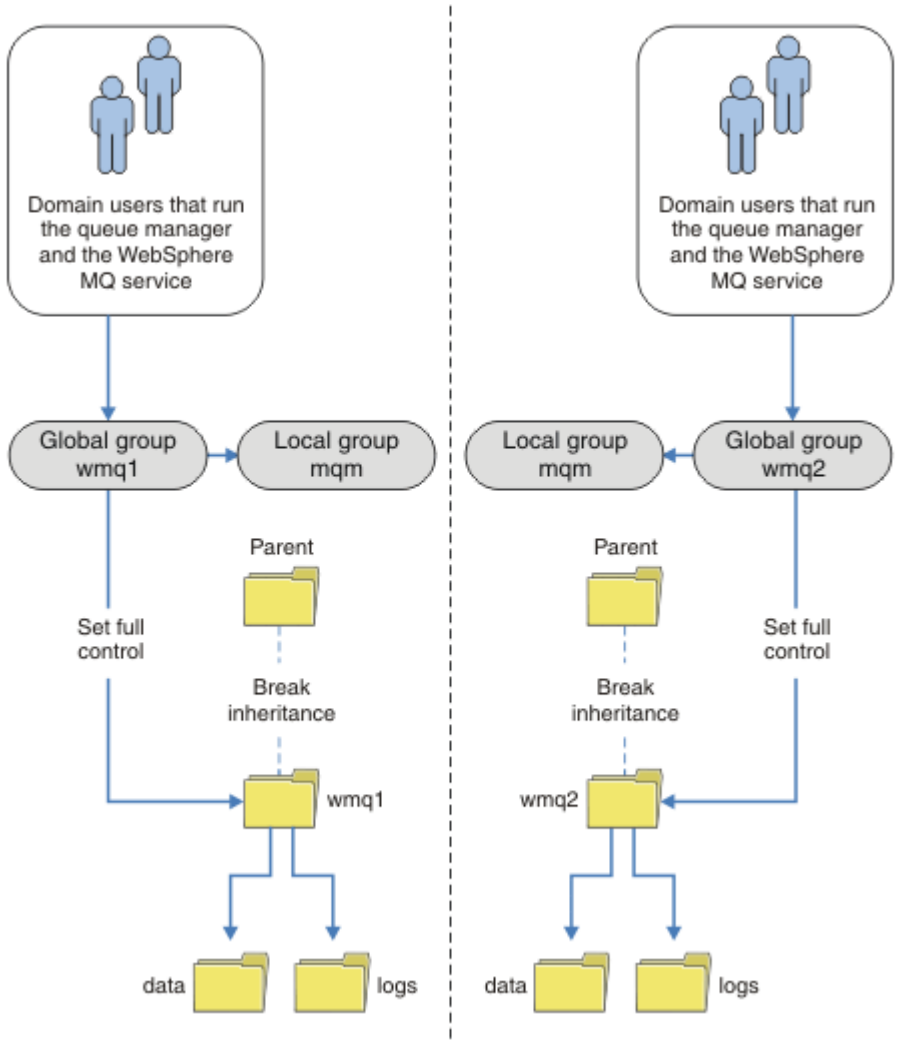
Obrázek 74. Zabezpečení dat a protokolů správce front pomocí alternativní globální skupiny zabezpečení (2)

Organizace v Obrázek 74 na stránce 525 je zbytečně komplikovaná. Uspořádání má dvě globální skupiny s identickými členy. Organizaci můžete zjednodušit a definovat pouze jednu globální skupinu; viz Obrázek 75 na stránce 525.



Obrázek 75. Zabezpečení dat a protokolů správce front pomocí alternativní globální skupiny zabezpečení (3)

Případně můžete potřebovat podrobnější řízení přístupu s různými správci front omezenými na přístup k různým složkám; viz Obrázek 76 na stránce 526. V produktu Obrázek 76 na stránce 526jsou definovány dvě skupiny uživatelů domény, v oddělených globálních skupinách pro zabezpečení různých protokolů správce front a datových souborů. Zobrazí se dvě různé lokální skupiny `mqm` , které musí být na různých serverech IBM MQ . V tomto příkladu jsou správci front rozděleni do dvou sad s různými uživateli, kteří jsou k těmto dvěma sadám přiděleni. Tyto dvě sady mohou být správci front pro testování a produkční. Alternativní skupiny zabezpečení se nazývají `wmq1` a `wmq2`. Globální skupiny `wmq1` a `wmq2` musíte ručně přidat do správných správců front podle toho, zda jsou v testovacím nebo produkčním oddělení. Konfigurace nemůže využít výhod, které instalace IBM MQ šíří `Domain mqm` do lokální skupiny `mqm` jako v Obrázek 75 na stránce 525, protože existují dvě skupiny uživatelů.



Obrázek 76. Zabezpečení dat a protokolů správce front pomocí alternativního globálního činitele zabezpečení (4)

Alternativním způsobem, jak rozdělit dvě oddělení, by bylo umístit je do dvou domén Windows. V takovém případě se můžete vrátit k použití jednoduššího modelu zobrazeného v souboru Obrázek 75 na stránce 525.

Windows *Zabezpečte nesdílená data a adresáře a soubory protokolů správce front 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 pomocí alternativní skupiny zabezpečení.

Obvykle nenastavujete alternativní umístění pro data správce front a soubory protokolu. Při instalaci produktu IBM MQ for Windowsinstalační program vytvoří domovský adresář podle vaší volby pro všechny vytvořené správce front. Zabezpečuje adresáře s lokální skupinou `mqm` a konfiguruje ID uživatele pro službu IBM MQ pro přístup k adresářům.

Dva příklady ukazují, jak nakonfigurovat řízení přístupu pro produkt IBM MQ. Příklady ukazují, jak vytvořit správce front s jeho daty a protokoly v adresářích, které nejsou v datech a cestách k protokolům vytvořených instalací. V prvním příkladu, “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 528, povolíte přístup k adresářům front a protokolů pomocí autorizace lokální skupiny `mqm` . Druhý příklad, “Čtení a zápis dat a souborů protokolu autorizovaných alternativní lokální skupinou zabezpečení” na stránce 531, se liší v tom, že přístup k adresářům je autorizován alternativní skupinou zabezpečení. Při přístupu k adresářům prostřednictvím správce front spuštěného pouze na jednom serveru vám zabezpečení dat a souborů protokolu pomocí alternativní skupiny

zabezpečení poskytuje možnost zabezpečení různých správců front s různými lokálními skupinami nebo činiteli. Při přístupu k adresářům prostřednictvím správce front spuštěného na různých serverech, například pomocí správce front s více instancemi, je jedinou volbou zabezpečení dat a souborů protokolu pomocí alternativní skupiny zabezpečení; viz “Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows” na stránce 523.

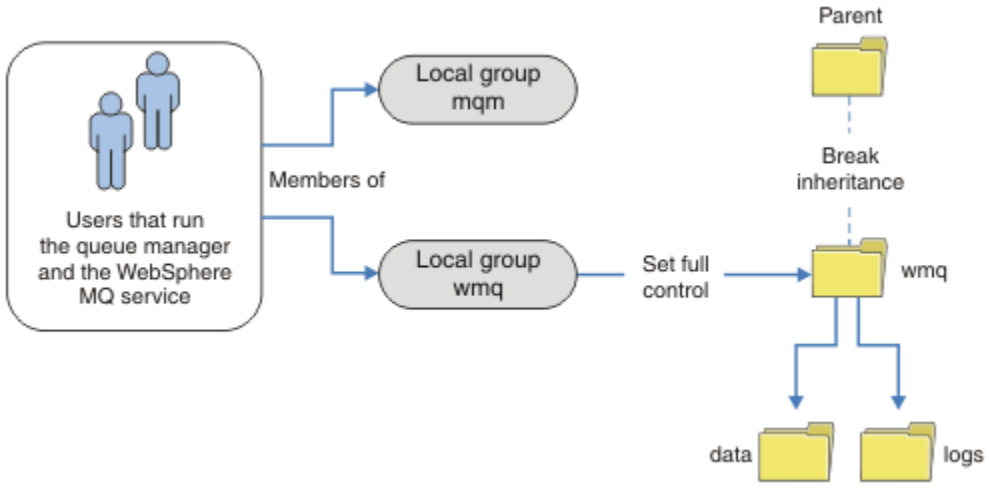
Konfigurace oprávnění zabezpečení dat správce front a souborů protokolu není v systému Windowsběžnou úlohou. Při instalaci produktu IBM MQ for Windowsbuď určíte adresáře pro data a protokoly správce front, nebo přijmete výchozí adresáře. Instalační program automaticky zabezpečí tyto adresáře pomocí lokální skupiny `mqm` a udělí jí plné oprávnění k řízení. Instalační proces zajišťuje, že ID uživatele, který spouští správce front, je členem lokální skupiny `mqm` . Ostatní přístupová oprávnění k adresářům můžete upravit tak, aby splňovala vaše požadavky na přístup.

Pokud přesunete adresář dat a souborů protokolu do nových umístění, musíte nakonfigurovat zabezpečení nových umístění. Umístění adresářů můžete změnit, pokud zálohujete správce front a obnovíte jej na jiný počítač nebo pokud změníte správce front na správce front s více instancemi. Máte na výběr ze dvou způsobů zabezpečení dat správce front a adresářů protokolu v novém umístění. Adresáře můžete zabezpečit tak, že omezíte přístup k lokální skupině `mqm` , nebo můžete omezit přístup k libovolné skupině zabezpečení dle vaší volby.

K zabezpečení adresářů pomocí lokální skupiny `mqm` je zapotřebí nejméně kroků. Nastavte oprávnění v datových adresářích a adresářích protokolů, abyste povolili úplné řízení lokální skupiny `mqm` . Typickým přístupem je zkopírovat existující sadu oprávnění a odebrat dědičnost z nadřízeného prvku. Poté můžete odebrat nebo omezit oprávnění jiných činitelů.

Pokud spustíte správce front pod jiným ID uživatele pro službu nastavenou v průvodci přípravou produktu IBM MQ , musí být toto ID uživatele členem lokální skupiny `mqm` . Úloha “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 528vás provede kroky.

Můžete také zabezpečit data správce front a soubory protokolu pomocí alternativní skupiny zabezpečení. Proces zabezpečení dat správce front a souborů protokolu pomocí alternativní skupiny zabezpečení obsahuje řadu kroků, které jsou uvedeny v tématu Obrázek 77 na stránce 527. Lokální skupina `wmq`je příkladem alternativní skupiny zabezpečení.



Obrázek 77. Zabezpečení dat a protokolů správce front 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, tak, že udělíte alternativní skupině `wmq`úplné oprávnění k řízení adresářů.
4. Poskytněte všem ID uživatelů, kteří spouštějí procesy správce front, pověření alternativní skupiny zabezpečení nebo činitele:
   a. Definujete-li uživatele jako alternativní činitel zabezpečení, musí být uživatel stejný jako ten, pod kterým bude spuštěn správce front. Uživatel musí být členem lokální skupiny `mqm` .
   b. Pokud definujete 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. Pokud definujete globální skupinu jako alternativní skupinu zabezpečení, prohlédněte si téma “Zabezpečení sdílených adresářů a souborů protokolů a dat správce front v systému Windows” na stránce 523.
5. Vytvořte správce front s uvedením alternativní skupiny zabezpečení nebo činitele v příkazu **crtmqm** s parametrem `-a` .

Windows *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 MQ for Windows jako primární instalaci.
2. Spusťte příkaz Prepare IBM MQ Wizard.

   Další informace viz Konfigurace IBM MQ s Prepare IBM MQ Wizard.

   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 “Domény Windows a správci front s více instancemi” na stránce 497, 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 “Domény Windows a správci front s více instancemi” na stránce 497.

V systému Windowsmůžete vytvořit výchozí cesty k datům a protokolům pro IBM 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 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 MQ konfigurována jako součást domény, učiňte ID uživatele členem skupiny `Domain mqm` . Průvodce "Připravit IBM 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:

```
IBM MQ queue manager created.
Directory 'c:\wmq\data\QMGR' created.
The queue manager is associated with installation '1'
Creating or replacing default objects for queue manager 'QMGR'
Default objects statistics : 74 created. 0 replaced.
Completing setup.
Setup completed.
```

6. Zkontrolujte, zda 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:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation '1'.
5 log records accessed on queue manager 'QMGR' during the log
```

```
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

2. Vytvořte testovací frontu.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

Odezva systému:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.  ALL RIGHTS RESERVED.
Starting MQSC for queue manager QMGR.


1 : define qlocal(QTEST)
AMQ8006: IBM MQ queue created.
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

3. Vložte testovací zprávu pomocí ukázkového programu **amqsput**.

```
echo 'A test message' | amqsput QTEST QMGR
```

Odezva systému:

```
Sample AMQSPUT0 start
target queue is QTEST
Sample AMQSPUT0 end
```

4. Získejte testovací zprávu pomocí ukázkového programu **amqsget**.

```
amqsget QTEST QMGR
```

Odezva systému:

```
Sample AMQSGET0 start
message A test message
Wait 15 seconds ...
no more messages
Sample AMQSGET0 end
```

5. Zastavte správce front.

```
endmqm -i QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

   Tip: Přidejte 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

“Domény Windows a správci front s více instancemi” na stránce 497
Správce front pro více instancí v systému Windows vyžaduje sdílení dat a protokolů. Sdílení musí být přístupné pro všechny instance správce front spuštěné na různých serverech nebo pracovních stanicích. Konfigurujte správce front a sdílejte je jako součást domény Windows . Správce front může být spuštěn na pracovní stanici nebo serveru domény nebo na řadiči domény.

Související úlohy

Windows 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.

“Čtení a zápis sdílených dat a souborů protokolu autorizovaných alternativní globální skupinou zabezpečení” na stránce 510
“Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows” na stránce 498

Windows *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 MQ for Windows jako primární instalaci.
2. Spusťte příkaz Prepare IBM MQ Wizard.

   Další informace viz Konfigurace IBM MQ s Prepare IBM MQ Wizard.

   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 “Domény Windows a správci front s více instancemi” na stránce 497, 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 “Domény Windows a správci front s více instancemi” na stránce 497.

V systému Windowsmůžete vytvořit výchozí cesty k datům a protokolům pro IBM 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 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 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 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 MQ .

      i) Klepněte na tlačítko **Spustit** > **Spustit ...**, Zadejte `services.msc` a klepněte na tlačítko **OK**.

      ii) Klepněte na službu IBM MQ v seznamu služeb a klepněte na kartu Přihlášení.

      iii) Zapamatujte si ID uživatele a zavřete průzkumník služeb.

   e) Přidejte ID uživatele, který spouští službu IBM MQ , do skupiny *altmqm* . Přidejte také ID uživatele, 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 MQ jako součást domény a chystáte se provést úlohy v produktu "Vytvoření správce front pro více instancí na pracovních stanicích domény nebo serverech v systému Windows" na stránce 498, ID uživatelů domény vytvořená v "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 501 jsou *wmquser1* a *wmquser2*.

      Pokud jste nenainstalovali správce front jako součást domény, výchozí ID lokálního uživatele, který spouští službu IBM 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) Do okna Zabezpečení Windows zadejte jméno a heslo administrátora domény a poté klepněte na tlačítko **OK** > **OK** > **Použít** > **OK**.

2. Otevřete příkazový řádek.
3. Restartujte službu IBM 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 MQ konfigurována jako součást domény, učiňte ID uživatele členem skupiny `Domain mqm` . Průvodce "Připravit IBM 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:

```
IBM MQ queue manager created.
Directory 'c:\wmq1\data\QMGR' created.
The queue manager is associated with installation '1'
Creating or replacing default objects for queue manager 'QMGR'
Default objects statistics : 74 created. 0 replaced.
Completing setup.
Setup completed.
```

8. Zkontrolujte, zda 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:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation '1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

2. Vytvořte testovací frontu.

```
echo define qlocal(QTEST) | runmqsc QMGR
```

   Odezva systému:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.  ALL RIGHTS RESERVED.
Starting MQSC for queue manager QMGR.


1 : define qlocal(QTEST)
AMQ8006: IBM MQ queue created.
One MQSC command read.
No commands have a syntax error.
All valid MQSC commands were processed.
```

3. Vložte testovací zprávu pomocí ukázkového programu **amqsput**.

```
echo 'A test message' | amqsput QTEST QMGR
```

   Odezva systému:

```
Sample AMQSPUT0 start
target queue is QTEST
Sample AMQSPUT0 end
```

4. Získejte testovací zprávu pomocí ukázkového programu **amqsget**.

```
amqsget QTEST QMGR
```

   Odezva systému:

```
Sample AMQSGET0 start
```

```
message A test message
Wait 15 seconds ...
no more messages
Sample AMQSGET0 end
```

5. Zastavte správce front.

```
endmqm -i QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended.
```

6. Odstraňte správce front.

```
dltmqm QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' deleted.
```

7. Odstraňte adresáře, které jste vytvořili.

Tip: Přidejte volbu /Q k příkazům, abyste zabránili náznaku příkazu k odstranění každého souboru nebo adresáře.

```
del /F /S C:\wmq\*.*
rmdir /S C:\wmq
```

Související úlohy

Windows 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.

Linux *Vytvoření správce front pro více instancí v systému Linux*
Příklad ukazující, jak nastavit správce front pro více instancí v systému Linux. Nastavení je malé pro ilustraci příslušných konceptů. Příklad je založen na systému Linux Red Hat Enterprise 5. Tyto kroky se liší na jiných platformách UNIX .

Informace o této úloze

Příklad je nastaven na přenosném počítači s frekvencí 2 GHz a 3 GB paměti RAM se systémem Windows 7 Service Pack 1. Dva virtuální počítače VMware , Server1 a Server2, spouští produkt Linux Red Hat Enterprise 5 v 640 MB obrazech. Server Server1 je hostitelem síťového systému souborů (NFS), protokolů správce front a instance HA. Není obvyklé, aby server NFS hostoval také jednu z instancí správce front; to zjednodušuje příklad. Server2 připojí protokoly správce front serveru Server1s rezervní instancí. Klient produktu WebSphere MQ MQI je nainstalován na dalším obrazu produktu VMware o velikosti 400 MB, který spouští produkt Windows 7 Service Pack 1 a spouští ukázkové aplikace s vysokou dostupností. Všechny virtuální počítače jsou z bezpečnostních důvodů nakonfigurovány jako součást sítě pouze pro hostitele VMware .

Poznámka: Na server NFS byste měli vložit pouze data správce front. V systému NFSpomocí následujících tří voleb příkazu mount zajistěte zabezpečení systému:

- **noexec**
  Pomocí této volby zastavíte spouštění binárních souborů na systému NFS, což zabrání vzdálenému uživateli ve spuštění nežádoucího kódu v systému.
- **nosuid**
  Pomocí této volby zabráníte použití bitů set-user-identifier a set-group-identifier, které brání vzdálenému uživateli získat vyšší oprávnění.
- **nodev**
  Pomocí této volby zastavíte použití nebo definování znakových a blokových speciálních zařízení, což zabrání vzdálenému uživateli dostat se z vězení chroot.

Postup

1. Přihlaste se jako uživatel root.
2. Přečtěte si téma Instalace IBM MQ -přehled a postupujte podle příslušného odkazu pro instalaci IBM MQ, vytvořte uživatele a skupinu mqm a definujte `/var/mqm`.
3. Dokončete úlohu Ověření chování sdíleného systému souborů a zkontrolujte, zda systém souborů podporuje správce front s více instancemi.
4. V případě serveru Server1postupujte takto:
   a. Vytvořte adresáře protokolu a dat ve společné složce `/MQHA`, která má být sdílena. Příklad:
      i) **mkdir** */MQHA*
      ii) **mkdir** */MQHA/logs*
      iii) **mkdir** */MQHA/qmgrs*
5. V případě serveru Server2postupujte takto:
   a. Vytvořte složku `/MQHA`pro připojení sdíleného systému souborů. Ponechte cestu stejnou jako na Server1. Příklad:
      i) **mkdir** */MQHA*
6. Ujistěte se, že adresáře `MQHA` vlastní uživatel a skupina mqm a přístupová oprávnění jsou pro uživatele a skupinu nastavena na hodnotu `rwx` . Například **ls -al** zobrazí `drwxrwxr-x mqm mqm 4096 Nov 27 14:38 MQDATA` .
   a. **chown -R** `mqm:mqm` */MQHA*
   b. **chmod -R** `ug+rwx` */MQHA*
7. Vytvořte správce front zadáním následujícího příkazu: **crtmqm -ld** */MQHA/logs* **-md** */MQHA/qmgrs QM1*
8. Přidat[2] `/MQHA *(rw,sync,no_wdelay,fsid=0)` na `/etc/exports`
9. V případě serveru Server1postupujte takto:
   a. Spusťte démona NFS : */etc/init.d/* **nfs** `start`
   b. Zkopírujte podrobnosti konfigurace 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
```

[2] Produkt '*' umožňuje všem počítačům, které mohou dosáhnout tohoto jediného připojení /MQHA pro čtení/zápis. Omezit přístup na produkčním počítači.

10. V případě serveru Server2postupujte takto:
    a. Připojte exportovaný systém souborů /MQHA zadáním následujícího příkazu: **mount -t** nfs4 **-o** hard,intr *Server1:/ /MQHA*
    b. Vložte příkaz pro konfiguraci správce front na server Server2:

```
 addmqinf -s QueueManager
-v Name=QM1
-v Directory=QM1
-v Prefix=/var/mqm
-v DataPath=/MQHA/qmgrs/QM1
```

11. Spusťte instance správce front v uvedeném pořadí s parametrem**-x** : **strmqm -x** QM1.

    Příkaz použitý ke spuštění instancí správce front musí být zadán ze stejné instalace produktu IBM MQ jako příkaz **addmqinf** . Chcete-li spustit a zastavit správce front z jiné instalace, musíte nejprve nastavit instalaci přidruženou ke správci front pomocí příkazu **setmqm** . Další informace viz setmqm.

Linux *Ověření správce front pro více instancí v systému Linux*

Pomocí ukázkových programů **amqsghac**, **amqsphac** a **amqsmhac** ověřte konfiguraci správce front pro více instancí. V tomto tématu je uveden příklad konfigurace pro ověření konfigurace správce front pro více instancí v systému Linux Red Hat Enterprise 5.

Ukázkové programy s vysokou dostupností používají automatické opětovné připojení klienta. Dojde-li k selhání připojeného správce front, klient se pokusí znovu připojit ke správci front ve stejné skupině správců front. Popis ukázek, Ukázkové programy vysoké dostupnosti, demonstruje opětovné připojení klienta pomocí jednoho správce front instance pro jednoduchost. Stejné ukázky můžete použít se správci front s více instancemi k ověření konfigurace správce front s více instancemi.

Příklad používá konfiguraci s více instancemi popsanou v části “Vytvoření správce front pro více instancí v systému Linux” na stránce 535. Pomocí konfigurace ověřte, že se správce front pro více instancí přepne na instanci v pohotovostním režimu. Zastavte správce front pomocí příkazu **endmqm** a použijte volbu -s, switchover,. Klientské programy se znovu připojí k nové instanci správce front a po malé prodlevě budou pokračovat v práci s novou instancí.

V tomto příkladu je klient spuštěn na systému Windows 7 Service Pack 1. Systém je hostitelem dvou serverů VMware Linux , na kterých je spuštěn správce front pro více instancí.

Ověření překonání selhání pomocí IBM MQ Explorer

Před použitím ukázkových aplikací k ověření překonání selhání spusťte IBM MQ Explorer na každém serveru. Přidejte obě instance správce front do každého průzkumníku pomocí průvodce **Přidat vzdáleného správce front > Připojit přímo ke správci front s více instancemi** . Ujistěte se, že jsou spuštěny obě instance, což umožňuje pohotovostní režim. Zavřete okno se spuštěným obrazem VMware s aktivní instancí, virtuálně vypněte server, nebo zastavte aktivní instanci, což umožní přepnutí na záložní instanci.

Poznámka: Pokud vypnete server, ujistěte se, že to není ten, který hostuje /MQHA !

Poznámka: Volba **Povolit přepnutí na rezervní instanci** nemusí být v dialogovém okně **Zastavit správce front** k dispozici. Tato volba chybí, protože správce front je spuštěn jako správce front s jednou instancí. Musíte ji spustit bez volby **Povolit instanci v pohotovostním režimu** . Je-li váš požadavek na zastavení správce front zamítnut, podívejte se do okna **Podrobnosti** . Možnou příčinou je, že není spuštěna žádná instance v pohotovostním režimu.

Ověření překonání selhání pomocí ukázkových programů

Zvolte server, který má být spuštěn pro aktivní instanci

Možná jste vybrali jeden ze serverů jako hostitele adresáře MQHA nebo systému souborů. Pokud plánujete testovat překonání selhání zavřením okna VMware , na kterém běží aktivní server, ujistěte se, že to není ten, který hostuje MQHA !

Na serveru, na kterém je spuštěna aktivní instance správce front.

Poznámka: Spuštění kanálu SVRCONN s volbou MCAUSER nastavenou na mqmje pohodlnější pro snížení počtu konfiguračních kroků v příkladu. Je-li vybráno jiné ID uživatele a váš systém je nastaven jinak než ten, který je použit v příkladu, může dojít k problémům s přístupovými oprávněními. Nepoužívejte mqm jako MCAUSER na vystaveném systému; je pravděpodobné, že značně ohrozí zabezpečení.

1. Upravte *ipaddr1* a *ipaddr2* a uložte následující příkazy v adresáři /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 spuštěn a zda má řízení správce front, a to buď kontrolou výstupu příkazu **runmqsc** .

```
LISTENER(LISTENER.TCP)CONTROL(QMGR)
LISTENER(LISTENER.TCP)STATUS(RUNNING)
```

   Nebo pomocí IBM MQ Explorer , že modul listener TCPIP je spuštěn a má Control = Queue Manager.

Na straně klienta

1. Zkopírujte tabulku připojení klienta AMQCLCHL.TAB z /MQHA/qmgrs/QM1.000/@ipcc na serveru do C:\ na klientovi.
2. Otevřete příkazový řádek s cestou C:\ a nastavte proměnnou prostředí MQCHLLIB tak, aby ukazovala na tabulku CCDT (Client Channel Definition Table).

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

3. Na příkazovém řádku 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 spuštěným obrazem VMware s aktivní instancí serveru.
   - Pomocí konzoly IBM MQ Explorerzastavte aktivní instanci správce front, čímž umožníte přepnutí na instanci v pohotovostním režimu a instruování klientů s možností opětovného připojení.
2. Tři klienti nakonec zjistí, že připojení je přerušeno, a pak se znovu připojí. Pokud v této konfiguraci zavřete okno serveru, trvá obnovení všech tří připojení přibližně sedm minut. Některá připojení jsou před ostatními znovu zavedena.

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
```

Multi *Odstranění správce front s více instancemi*

Chcete-li na platformě Multiplatforms zcela odstranit správce front s více instancemi, použijte příkaz **dltmqm** k odstranění správce front a poté odeberte instance z jiných serverů pomocí příkazů **rmvmqinf** nebo **dltmqm** .

Spuštěním příkazu **dltmqm** odstraňte správce front, který má instance definované na jiných serverech, na libovolném serveru, na kterém je daný správce front definován. Příkaz **dltmqm** nemusíte spouštět 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 lze odstranit pouze v případě, že je zastaven. V době, kdy ji odstraníte, nejsou spuštěny žádné instance a správce front, přesně řečeno, není ani jedním správcem front, ani správcem front s více instancemi; jedná se pouze o správce front, který má svá data správce front a protokoly ve vzdálené sdílené složce. Když odstraníte správce front, jeho data a protokoly správce front se odstraní a sekce správce front se odebere ze souboru `mqs.ini` na serveru, na kterém jste zadali příkaz **dltmqm** . Při odstraňování správce front musíte mít přístup k síťovému sdílení obsahujícímu data a protokoly správce front.

Na jiných serverech, na kterých jste dříve vytvořili instance správce front, jsou také položky v souborech `mqs.ini` na těchto serverech. Postupně je třeba navštívit každý server a odebrat sekci správce front spuštěním příkazu **rmvmqinf** *Název sekce správce front*.

Linux AIX Pokud jste v systémech AIX and Linux umístili do síťového úložiště společný soubor `mqs.ini` a odkázali na něj ze všech serverů nastavením proměnné prostředí `AMQ_MQS_INI_LOCATION` na každém serveru, musíte odstranit správce front pouze z jednoho z jeho serverů, protože existuje pouze jeden soubor `mqs.ini` , který se má aktualizovat.

Příklad

První server

dltmqm QM1

Jiné servery, na kterých jsou definovány instance

rmvmqinf QM1 nebo

dltmqm QM1

Multi *Spuštění a zastavení správce front pro více instancí*

Spuštění a zastavení správce front konfigurovaného na platformě Multiplatforms buď jako jedna instance, nebo jako správce front s více instancemi.

Pokud jste definovali správce front s více instancemi na dvojici serverů, můžete správce front spustit buď na serveru, buď jako správce front s jednou instancí, nebo jako správce front s více instancemi.

Chcete-li spustit správce front s více instancemi, spusťte jej na jednom ze serverů pomocí příkazu **strmqm** -x *QM1* ; volba -x umožňuje instanci provést překonání selhání. Stane se *aktivní instancí*. Spusťte záložní instanci na jiném serveru pomocí stejného příkazu **strmqm** -x *QM1* ; volba -x umožňuje spuštění instance jako záložní.

Správce front je nyní spuštěn s jednou aktivní instancí, která zpracovává všechny požadavky, a rezervní instancí, která je připravena převzít v případě selhání aktivní instance. Aktivní instanci je udělen výlučný přístup k datům a protokolům správce front. Rezervní databáze čeká na udělení výlučného přístupu k datům a protokolům správce front. Když je rezervní databázi udělen výlučný přístup, stane se aktivní instancí.

Řízení můžete také ručně přepnout na rezervní instanci zadáním příkazu **endmqm** -s na aktivní instanci. Příkaz **endmqm** -s ukončí aktivní instanci bez ukončení pohotovostního režimu. Zámek výlučného přístupu pro data a protokoly správce front je uvolněn a rezervní databáze jej převezme.

Můžete také spustit a zastavit správce front konfigurovaného s více instancemi na různých serverech jako správce front s jednou instancí. Pokud spustíte správce front bez použití volby -x v příkazu **strmqm** , instance správce front nakonfigurované v jiných počítačích nebudou moci spouštět jako instance v pohotovostním režimu. Pokusíte-li se spustit jinou instanci, obdržíte odpověď, že instance správce front nemá povolení ke spuštění v pohotovostním režimu.

Pokud zastavíte aktivní instanci správce front s více instancemi pomocí příkazu **endmqm** bez volby -s , budou aktivní i rezervní instance zastavené. Pokud zastavíte rezervní instanci pomocí příkazu **endmqm** s volbou -x , přestane být rezervní a aktivní instance bude pokračovat ve spuštění. Nemůžete vydat příkaz **endmqm** bez volby -x na rezervní databázi.

Současně mohou být spuštěny pouze dvě instance správce front; jedna je aktivní instance a druhá je instance v pohotovostním režimu. Spustíte-li současně dvě instance, produkt IBM MQ nemá žádnou kontrolu nad tím, která instance se stane aktivní instancí; je určena síťovým systémem souborů. První instance, která získá výhradní přístup k datům správce front, se stane aktivní instancí.

Poznámka: Před restartováním nezdařeného správce front je nutné odpojit aplikace od této instance správce front. Pokud tak neučiníte, nemusí být správce front správně restartován.

Multi *Sdílený systém souborů*

Na platformě Mulitplatforms používá správce front s více instancemi ke správě instancí správce front systém souborů v síti.

Správce front s více instancemi automatizuje překonání selhání pomocí kombinace zámků systému souborů a sdílených dat a protokolů správce front. Pouze jedna instance správce front může mít výlučný

přístup k datům a protokolům sdíleného správce front. Jakmile získá přístup, stane se aktivní instancí. Druhá instance, které se nepodařilo získat výhradní přístup, čeká jako rezervní instance, dokud nebudou data a protokoly správce front k dispozici.

Síťový systém souborů je odpovědný za uvolnění zámků, které zadržuje pro aktivní instanci správce front. Pokud aktivní instance nějakým způsobem selže, síťový systém souborů uvolní zámky, které zadržuje pro aktivní instanci. Jakmile je výlučný zámek uvolněn, správce front v pohotovostním režimu čeká na pokus o jeho získání. V případě úspěchu se stane aktivní instancí a bude mít výhradní přístup k datům správce front a protokolům ve sdíleném systému souborů. Pak pokračuje ve spouštění.

Související téma Plánování podpory systému souborů popisuje, jak 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 řada způsobů, jak chránit vaše data.

- Investujte do spolehlivého úložiště, jako jsou pole RAID (redundant disk arrays), a začleňte je do síťového systému souborů, který je odolný vůči síti.
- Zazálohujte lineární protokoly IBM MQ na alternativní médium, a pokud dojde k selhání média primárního protokolu, proveďte obnovu pomocí protokolů na alternativním médiu. K administraci tohoto procesu můžete použít záložního správce front.

Multi *Více instancí správce front*

Správce front s více instancemi je schopný obnovy, protože používá instanci správce front v pohotovostním režimu k obnovení dostupnosti správce front po selhání.

Replikace instancí správce front je velmi efektivní způsob, jak zlepšit dostupnost procesů správce front. Použití jednoduchého modelu dostupnosti, čistě pro ilustraci: pokud je spolehlivost jedné instance správce front 99% (za jeden rok, kumulativní prostoj je 3.65 dnů), pak přidání další instance správce front zvýší dostupnost na 99.99% (za jeden rok, kumulativní prostoj přibližně za hodinu).

Tento model je příliš jednoduchý na to, aby vám poskytl praktické číselné odhady dostupnosti. Chcete-li realisticky modelovat dostupnost, musíte shromáždit statistiku pro střední dobu mezi selháními (MTBF) a střední dobu opravy (MTTR) a pravděpodobnostní rozložení času mezi selháními a dobou opravy.

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 chrání před selháním procesů správce front tím, že mají jednu instanci správce front aktivní na jednom serveru a jinou instanci správce front v pohotovostním režimu na jiném serveru, které jsou připraveny převzít řízení automaticky v případě selhání aktivní instance.

Multi *Překonání selhání nebo přepnutí*

Instance správce front v pohotovostním režimu přebírá od aktivní instance buď na vyžádání (přepnutí), nebo při selhání aktivní instance (překonání selhání).

- *Přepnutí* se provede při spuštění rezervní instance v reakci na příkaz **endmqm** `-s` , který byl zadán pro aktivní instanci správce front. Můžete uvést **endmqm** parametry `-c`, `-i` nebo `-p` , chcete-li řídit, jak náhle je správce front zastaven.

  Poznámka: K přepnutí dochází 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 pohotovostního správce front.
- *Překonání selhání* se vyskytne, když je zámek na datech správce front zadržených aktivní instancí uvolněn, protože se instance neočekávaně zastavila (tj. bez zadání příkazu **endmqm**).

Když rezervní instance převezme funkci aktivní instance, zapíše zprávu do protokolu chyb správce front.

Klienti s možností opětovného připojení jsou automaticky znovu připojeni v případě, že dojde k selhání správce front nebo k přepnutí. Nemusíte zahrnout příznak `-r` do příkazu **endmqm** , chcete-li požadovat opětovné připojení klienta. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Pokud zjistíte, že nemůžete restartovat nezdařenou instanci, i když došlo k překonání selhání a instance v pohotovostním režimu se stala aktivní, zkontrolujte, zda se aplikace lokálně připojené k nezdařené instanci odpojily od nezdařené instance.

Lokálně připojené aplikace musí skončit nebo se odpojit od nezdařené instance správce front, aby mohla být instance, která selhala, restartována. Všechny lokálně připojené aplikace používající sdílené vazby (což je výchozí nastavení), které zadržují připojení k nezdařené instanci, aby zabránily restartování instance.

Pokud není možné ukončit lokálně připojené aplikace nebo se ujistit, že se při selhání lokální instance správce front odpojí, zvažte použití izolovaných vazeb. Lokálně připojené aplikace používající izolované vazby nebrání restartování lokální instance správce front, a to ani v případě, že se neodpojují.

Multi *Opětovné připojení kanálu a klienta*

Opětovné připojení kanálu a klienta je nezbytnou součástí obnovy zpracování zpráv po aktivaci instance správce front v pohotovostním režimu.

Instance správce front s více instancemi jsou instalovány na serverech s různými síťovými adresami. Musíte nakonfigurovat kanály a klienty IBM MQ s informacemi o připojení pro všechny instance správce front. Při převzetí pohotovostního režimu jsou klienti a kanály automaticky znovu připojeni k nově aktivní instanci správce front na nové síťové adrese. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Návrh se liší od způsobu, jakým prostředí s vysokou dostupností, jako je například práce HA-CMP. HA-CMP poskytuje virtuální adresu IP pro klastr a přenáší adresu na aktivní server. IBM MQ reconnection nemění ani nepřesměrovává adresy IP. Funguje tak, že se znovu připojí pomocí síťových adres, které jste definovali v definicích kanálů a připojení klienta. 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 seznam názvů připojení oddělených čárkami; například `CONNAME('127.0.0.1(1234), 192.0.2.0(4321)')`. Připojení se zkoušejí v pořadí uvedeném v seznamu připojení, dokud nebude připojení úspěšně zavedeno. Není-li připojení úspěšné, kanál se pokusí znovu připojit.

Kanály klastru

Pro práci správců front s více instancemi v klastru obvykle není vyžadována žádná další konfigurace.

Pokud se správce front připojí ke správci front úložiště, úložiště zjistí síťovou adresu správce front. Odkazuje na `CONNAME` kanálu `CLUSRCVR` ve správci front. V protokolu TCPIP správce front automaticky nastaví hodnotu `CONNAME` , pokud ji vynecháte, nebo ji nakonfigurujete na mezery. Když instance v pohotovostním režimu převezme kontrolu, její adresa IP nahradí adresu IP předchozí aktivní instance jako `CONNAME`.

Je-li to nezbytné, můžete ručně konfigurovat `CONNAME` se seznamem síťových adres instancí správce front.

Připojení klienta
Klientská připojení mohou používat seznamy připojení nebo skupiny správců front k výběru alternativních připojení.

Když dojde k překonání selhání, opětovné připojení trvá určitou dobu. Záložní správce front musí dokončit své spuštění. Klienti připojení ke správci front, který selhal, musí zjistit selhání připojení a spustit nové připojení klienta. Pokud nové připojení klienta vybere záložního správce front, který se stal nově aktivním, bude klient znovu připojen ke stejnému správci front.

Pokud se klient nachází uprostřed volání MQI během opětovného připojení, musí před dokončením volání tolerovat rozšířené čekání.

Dojde-li k selhání během dávkového přenosu v kanálu zpráv, je dávka odvolána a restartována.

Přepnutí je rychlejší než přepnutí při selhání a trvá pouze po dobu zastavení jedné instance správce front a spuštění jiné. V případě správce front, který má pouze několik záznamů protokolu k přehrání, může přepnutí trvat několik sekund. Chcete-li odhadnout, jak dlouho trvá překonání selhání, musíte přidat čas, který trvá zjištění selhání. V nejlepším případě detekce trvá 10 sekund a může trvat několik minut, v závislosti na síti a systému souborů.

Multi *Obnova aplikace*

Obnova aplikace je automatizované pokračování zpracování aplikace po překonání selhání. Zotavení aplikace po překonání selhání vyžaduje pečlivý návrh. Některé aplikace musí mít na paměti, že došlo k překonání selhání.

Cílem obnovy aplikace je, aby aplikace pokračovala ve zpracování pouze s krátkou prodlevou. Než budete pokračovat v novém zpracování, musí aplikace vrátit zpět a znovu odeslat pracovní jednotku, kterou zpracovala během selhání.

Problém při zotavení aplikace spočívá ve ztrátě kontextu, který je sdílen mezi produktem IBM MQ MQI client a správcem front a uložen ve správci front. Produkt IBM MQ MQI client obnoví většinu kontextu, ale existují některé části kontextu, které nelze spolehlivě obnovit. V následujících oddílech jsou popsány některé vlastnosti zotavení aplikace a jejich vliv na obnovu aplikací připojených ke správci front s více instancemi.

Transakční zasílání zpráv

Z hlediska doručování zpráv se při překonání selhání nemění trvalé vlastnosti systému zpráv IBM MQ . Pokud jsou zprávy trvalé a jsou správně spravovány v rámci pracovních jednotek, nejsou zprávy během překonání selhání ztraceny.

Z hlediska zpracování transakcí jsou transakce po překonání selhání buď vráceny zpět, nebo potvrzeny.

Nepotvrzené transakce jsou odvolány. Po překonání selhání znovu připojitelná aplikace obdrží kód příčiny `MQRC_BACKED_OUT` , který označuje, že transakce selhala. Poté je třeba transakci znovu restartovat.

Potvrzené transakce jsou transakce, které dosáhly druhé fáze dvoufázového potvrzování, nebo jednofázové (pouze zprávy) transakce, které zahájily `MQCMIT`.

Pokud je správcem front koordinátor transakcí a produkt `MQCMIT` zahájil druhou fázi dvoufázového potvrzování před selháním, transakce se úspěšně dokončí. Dokončení je pod kontrolou správce front a pokračuje, když je správce front znovu spuštěn. V opětovně připojitelné aplikaci se volání `MQCMIT` dokončí normálně.

V jednofázovém potvrzování, které zahrnuje pouze zprávy, se transakce, která spustila zpracování potvrzení, dokončí po opětovném spuštění normálně pod kontrolou správce front. V opětovně připojitelné aplikaci se `MQCMIT` dokončí normálně.

Klienti s možností opětovného připojení mohou jako koordinátor transakcí používat jednofázové transakce pod kontrolou správce front. Rozšířený transakční klient nepodporuje opětovné připojení. Je-li vyžadováno opětovné připojení při připojení klienta transakce, připojení bude úspěšné, ale bez možnosti opětovného připojení. Připojení se chová, jako by nebylo znovu připojitelné.

Restart aplikace nebo pokračování

Překonání selhání přeruší aplikaci. Po selhání se může aplikace restartovat od začátku, nebo může pokračovat ve zpracování po přerušení. Druhý z nich se nazývá *automatické opětovné připojení klienta*. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Pomocí aplikace IBM MQ MQI client můžete nastavit volbu připojení pro automatické opětovné připojení klienta. Volby jsou `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR`. Není-li nastavena žádná volba, klient se nepokusí znovu automaticky připojit a selhání správce front vrátí klientovi hodnotu `MQRC_CONNECTION_BROKEN` . Můžete navrhnout klienta, aby se pokusil spustit nové připojení zadáním nového volání `MQCONN` nebo `MQCONNX` .

Serverové programy je třeba restartovat; správce front je nemůže automaticky znovu připojit v okamžiku, kdy byly zpracovány, když došlo k selhání správce front nebo serveru. Programy serveru IBM MQ se v případě selhání instance správce front pro více instancí obvykle v záložní instanci správce front nerestartují.

Program serveru IBM MQ můžete automatizovat, aby se restartoval na záložním serveru, a to dvěma způsoby:

1. Zabalte serverovou aplikaci jako službu správce front. Restartuje se při restartování správce front v pohotovostním režimu.
2. Zapište vlastní logiku překonání selhání, spuštěnou například zprávou protokolu překonání selhání zapsanou instancí správce front v pohotovostním režimu při spuštění. Instance aplikace pak musí po spuštění volat MQCONN nebo MQCONNX , aby vytvořila připojení ke správci front.

Zjišťování překonání selhání

Některé aplikace si musí být vědomy překonání selhání, jiné ne. Zvažte tyto dva příklady.

1. Aplikace systému zpráv, která získává nebo přijímá zprávy prostřednictvím kanálu systému zpráv, obvykle nevyžaduje, aby byl spuštěn správce front na druhém konci kanálu: je nepravděpodobné, že by byl ovlivněn, pokud se správce front na druhém konci kanálu restartuje v rezervní instanci.
2. Aplikace IBM MQ MQI client zpracovává vstup trvalých zpráv z jedné fronty a vkládá odpovědi trvalých zpráv do jiné fronty jako součást jediné pracovní jednotky: pokud zpracovává MQRC_BACKED_OUT kód příčiny z MQPUT, MQGET nebo MQCMIT v synchronizačním bodu restartováním jednotky práce, nebudou ztraceny žádné zprávy. Aplikace navíc nemusí provádět žádné speciální zpracování, aby se vypořádala se selháním připojení.

Ve druhém příkladu však předpokládejme, že aplikace prochází frontu a vybírá zprávu ke zpracování pomocí volby MQGET MQGMO_MSG_UNDER_CURSOR. Opětovné připojení resetuje kurzor procházení a volání MQGET nevrátí správnou zprávu. V tomto příkladu musí aplikace vědět, že došlo k překonání selhání. Před vydáním dalšího souboru MQGET pro zprávu pod kurzorem musí aplikace navíc obnovit kurzor procházení.

Ztráta kurzoru procházení je jedním z příkladů změn kontextu aplikace po opětovném připojení. Ostatní případy jsou zdokumentovány v souboru “Obnova automaticky znovu připojeného klienta” na stránce 545.

Máte tři alternativní návrhové vzory pro aplikace IBM MQ MQI client po překonání selhání. Pouze jeden z nich nemusí zjistit překonání selhání.

Bez opětovného připojení

V tomto vzoru aplikace zastaví veškeré zpracování aktuálního připojení, když je připojení přerušeno. Aby mohla aplikace pokračovat ve zpracování, musí vytvořit nové připojení ke správci front. Aplikace je plně zodpovědná za přenos všech informací o stavu, které vyžaduje, aby mohla pokračovat ve zpracování nového připojení. Tímto způsobem jsou zapsány existující klientské aplikace, které se znovu připojí ke správci front po ztrátě připojení.

Klient obdrží kód příčiny, například MQRC_CONNECTION_BROKENnebo MQRC_Q_MGR_NOT_AVAILABLE , z dalšího volání MQI po ztrátě připojení. Aplikace musí vyřadit všechny své informace o stavu IBM MQ , jako jsou popisovače fronty, a vydat nové volání MQCONN nebo MQCONNX , aby navázala nové připojení, a poté znovu otevřít objekty IBM MQ , které potřebuje zpracovat.

Výchozí chování MQI spočívá v tom, že manipulátor připojení správce front bude po ztrátě připojení ke správci front nepoužitelný. Výchozí nastavení je ekvivalentní nastavení volby MQCNO_RECONNECT_DISABLED v systému MQCONNX , aby se zabránilo opětovnému připojení aplikace po překonání selhání.

Tolerantní k překonání selhání

Zapište aplikaci tak, aby ji neovlivnilo překonání selhání. Někdy je pro překonání selhání dostatečné pečlivé ošetření chyb.

S ohledem na opětovné připojení

Registrujte obslužnou rutinu událostí MQCBT_EVENT_HANDLER se správcem front. Obslužná rutina událostí se odešle spolu s produktem MQRC_RECONNECTING , když se klient začne pokoušet o opětovné připojení k serveru, a s produktem MQRC_RECONNECTED po úspěšném opětovném připojení. Poté můžete spustit rutinu, která znovu vytvoří předvídatelný stav, aby mohla klientská aplikace pokračovat ve zpracování.

Obnova automaticky znovu připojeného klienta

Překonání selhání je neočekávaná událost a aby automaticky znovu připojený klient fungoval podle návrhu, musí být důsledky opětovného připojení předvídatelné.

Hlavním prvkem přeměny neočekávaného selhání na předvídatelné a spolehlivé zotavení je použití transakcí.

V předchozí sekci byl uveden příklad, “2” na stránce 544, IBM MQ MQI client používající lokální transakci ke koordinaci MQGET a MQPUT. Klient vydá volání MQCMIT nebo MQBACK v reakci na chybu MQRC_BACKED_OUT a poté znovu odešle odvolanou transakci. Selhání správce front způsobí odvolání transakce a chování klientské aplikace zajistí, že nebudou ztraceny žádné transakce a žádné zprávy.

Všimněte si, že pro zpětné volání může být nezbytné pokračovat v odběratelské aplikaci, pokud je stav parametru spotřebitele zpětného volání: MQCS_SUSPENDED_USER_ACTION.

Ne všechny stavy programu jsou spravovány jako součást transakce, a proto je těžší porozumět důsledkům opětovného připojení. Potřebujete vědět, jak opětovné připojení změní stav IBM MQ MQI client , aby bylo možné navrhnout aplikaci klienta tak, aby přežila překonání selhání správce front.

Můžete se rozhodnout navrhnout aplikaci bez použití speciálního kódu pro překonání selhání, který bude zpracovávat chyby opětovného připojení se stejnou logikou jako ostatní chyby. Alternativně se můžete rozhodnout, že opětovné připojení vyžaduje speciální zpracování chyb, a zaregistrovat obslužnou rutinu událostí s produktem IBM MQ , která spustí rutinu pro zpracování překonání selhání. Rutina může zpracovat samotné zpracování opětovného připojení nebo nastavit příznak, který hlavnímu podprocesu programu označí, že když pokračuje ve zpracování, musí provést zpracování obnovy.

Prostředí IBM MQ MQI client si je vědomo samotného překonání selhání a obnovuje kontext v co největší míře po opětovném připojení uložením některých informací o stavu v klientu a zadáním dalších volání MQI jménem aplikace klienta za účelem obnovení stavu IBM MQ . Jsou například obnoveny popisovače objektů, které byly otevřeny v místě selhání, a dočasné dynamické fronty jsou otevřeny se stejným názvem. Ale existují změny, které jsou nevyhnutelné a vy potřebujete svůj návrh, abyste se s těmito změnami vypořádali. Změny lze rozdělit do pěti druhů:

1. Volání MQI vrací nové nebo dříve nediagnostikované chyby, dokud aplikační program neobnoví konzistentní nový stav kontextu.

   Příkladem přijetí nové chyby je návratový kód MQRC_CONTEXT_NOT_AVAILABLE při pokusu o předání kontextu po uložení kontextu před opětovným připojením. Kontext nelze po opětovném připojení obnovit, protože kontext zabezpečení není předán neautorizovanému klientskému programu. Chcete-li tak učinit, nechte škodlivý aplikační program získat kontext zabezpečení.

   Aplikace obvykle zpracovávají běžné a předvídatelné chyby pečlivě navrženým způsobem a odsunují neobvyklé chyby do generické obslužné rutiny chyb. Obslužná rutina chyb se může odpojit od produktu IBM MQ a znovu se připojit, nebo dokonce zastavit program úplně. Chcete-li zlepšit kontinuitu, možná budete muset řešit některé chyby jiným způsobem.
2. Dočasné zprávy mohou být ztraceny.
3. Transakce jsou odvolány (což může také pozastavit asynchronní spotřebitele, viz předchozí text).
4. Volání MQGET nebo MQPUT použitá mimo synchronizační bod mohou být přerušena možnou ztrátou zprávy.
5. Časování vyvolalo chyby v důsledku delšího čekání ve volání MQI.

Některé podrobnosti o ztraceném kontextu jsou uvedeny v následující sekci.

- Dočasné zprávy jsou vyřazeny, pokud nejsou vloženy do fronty s volbou NPMCLASS (HIGH) a selhání správce front nepřerušilo volbu ukládání dočasných zpráv při ukončení práce systému.
- Při přerušení připojení dojde ke ztrátě netrvalého odběru. Při opětovném připojení se znovu ustanoví. Zvažte použití trvalého odběru.
- Interval čekání na získání se přepočítá; pokud je jeho limit překročen, vrátí hodnotu MQRC_NO_MSG_AVAILABLE. Podobně je vypršení platnosti předplatného přepočítáno tak, aby poskytovala stejnou celkovou dobu vypršení platnosti.
- Pozice kurzoru procházení ve frontě je ztracena; obvykle je znovu zavedena před první zprávou.
  - Volání systému MQGET , která určují volbu MQGMO_BROWSE_MSG_UNDER_CURSOR nebo MQGMO_MSG_UNDER_CURSOR, selžou s kódem příčiny MQRC_NO_MSG_AVAILABLE.
  - Zprávy zamčené pro procházení jsou odemčené.
  - Procházet označené zprávy s rozsahem popisovače jsou neoznačené a lze je znovu procházet.
  - Ve většině případů je neoznačeno kooperativní procházení označených zpráv.
- Kontext zabezpečení je ztracen. Pokusí se použít uložený kontext zprávy, například vložení zprávy s MQPMO_PASS_ALL_CONTEXT se nezdařilo s MQRC_CONTEXT_NOT_AVAILABLE.
- Tokeny zpráv jsou ztraceny. MQGET použití tokenu zprávy vrací kód příčiny MQRC_NO_MSG_AVAILABLE.

  Poznámka: *MsgId* a *CorrelId*, protože jsou součástí zprávy, jsou zachovány se zprávou během překonání selhání, a proto MQGET použití MsgId nebo CorrelId funguje podle očekávání.
- Zprávy vložené do fronty v synchronizačním bodu v nepotvrzené transakci již nejsou k dispozici.
- Zpracování zpráv v logickém pořadí nebo ve skupině zpráv vede po opětovném připojení k návratovému kódu MQRC_RECONNECT_INCOMPATIBLE .
- Volání MQI může vrátit hodnotu MQRC_RECONNECT_FAILED spíše než obecnější hodnotu MQRC_CONNECTION_BROKEN , kterou klienti obvykle přijímají dnes.
- Opětovné připojení během volání MQPUT mimo synchronizační bod vrátí hodnotu MQRC_CALL_INTERRUPTED , pokud agent IBM MQ MQI client neví, zda byla zpráva úspěšně doručena správci front. Opětovné připojení během MQCMIT se chová podobně.
- Funkce MQRC_CALL_INTERRUPTED je vrácena-po úspěšném opětovném připojení-v případě, že konzola IBM MQ MQI client neobdržela od správce front žádnou odpověď, která by označovala úspěch nebo selhání
  - doručení trvalé zprávy pomocí volání MQPUT mimo synchronizační bod.
  - doručení trvalé zprávy nebo zprávy s výchozí perzistencí pomocí volání MQPUT1 mimo synchronizační bod.
  - potvrzení transakce pomocí volání MQCMIT. Odpověď je vrácena pouze po úspěšném opětovném připojení.
- Kanály jsou restartovány jako nové instance (mohou být také různými kanály), a proto není zachován žádný stav uživatelské procedury kanálu.
- Dočasné dynamické fronty jsou obnoveny jako součást procesu obnovy klientů s možností opětovného připojení, kteří měli otevřené dočasné dynamické fronty. Nejsou obnoveny žádné zprávy v dočasné dynamické frontě, ale aplikace, které měly otevřenou frontu nebo si zapamatovaly název fronty, jsou schopny pokračovat ve zpracování.

  Existuje možnost, že pokud je fronta používána jinou aplikací než tou, která ji vytvořila, nemusí být obnovena dostatečně rychle, aby byla přítomna při dalším odkazování. Pokud například klient vytvoří dočasnou dynamickou frontu jako frontu pro odpověď a kanál umístí zprávu odpovědi do fronty, nemusí být tato fronta včas obnovena. V tomto případě by kanál obvykle umístil zprávu odpovědi na zprávu do fronty nedoručených zpráv.

  Pokud znovu připojitelná klientská aplikace otevře dočasnou dynamickou frontu podle názvu (protože ji již vytvořila jiná aplikace), pak při opětovném připojení nemůže produkt IBM MQ MQI client znovu vytvořit dočasnou dynamickou frontu, protože nemá model, ze kterého by ji mohl vytvořit. V rozhraní MQI může dočasnou dynamickou frontu otevřít pouze jedna aplikace podle modelu. Jiné aplikace, které

chtějí používat dočasnou dynamickou frontu, musí používat MQPUT1nebo vazby serveru, nebo musí mít možnost zopakovat pokus o opětovné připojení, pokud se nezdaří.

Do dočasné dynamické fronty mohou být vloženy pouze dočasné zprávy a tyto zprávy jsou během překonání selhání ztraceny. Tato ztráta platí pro zprávy vkládané do dočasné dynamické fronty pomocí příkazu MQPUT1 během opětovného připojení. Dojde-li během operace MQPUT1k překonání selhání, je možné, že zpráva nebude vložena, ačkoli příkaz MQPUT1 uspěje. Jedním z náhradního řešení tohoto problému je použití trvalých dynamických front. Dočasnou dynamickou frontu může otevřít libovolná aplikace vazeb serveru podle názvu, protože ji nelze znovu připojit.

Multi *Obnova dat a vysoká dostupnost*

Řešení vysoké dostupnosti používající správce front s více instancemi musí obsahovat mechanizmus pro obnovu dat po selhání úložiště.

Správce front s více instancemi zvyšuje dostupnost procesů správce front, nikoli však dostupnost jiných komponent, například systému souborů, který správce front používá k ukládání zpráv, a dalších informací.

Jedním ze způsobů, jak zajistit vysokou dostupnost dat, je používat odolné datové úložiště připojené na síť. Buď můžete vytvořit vlastní řešení pomocí síťového systému souborů a odolného datového úložiště, nebo si můžete zakoupit integrované řešení. Chcete-li kombinovat odolnost s obnovou po havárii, je k dispozici asynchronní replikace disku, která umožňuje replikaci disku v desítkách nebo stovkách kilometrů.

Můžete nakonfigurovat způsob, jakým jsou různé adresáře IBM MQ mapovány na úložné médium, aby se co nejlépe využila média. Pro správce front *s více instancemi* existuje důležitý rozdíl mezi dvěma typy adresářů a souborů IBM MQ .

Adresáře, které musí být sdíleny mezi instancemi správce front.
Informace, které musí být sdíleny mezi různými instancemi správce front, jsou ve dvou adresářích: v adresářích `qmgrs` a `logs` . Adresáře musí být ve sdíleném síťovém systému souborů. Doporučuje se používat úložné médium, které poskytuje nepřetržitou vysokou dostupnost a vynikající výkon, protože data se neustále mění při vytváření a odstraňování zpráv.

Adresáře a soubory, které *nemají* pro sdílení mezi instancemi správce front.
Některé další adresáře nemusí být sdíleny mezi různými instancemi správce front a jsou rychle obnoveny jinými prostředky než pomocí zrcadleného systému souborů.

- Spustitelné soubory IBM MQ a adresář nástrojů. Nahraďte přeinstalováním nebo zálohováním a obnovením ze zálohovaného archivu souborů.
- Informace o konfiguraci, které jsou upraveny pro instalaci jako celek. Informace o konfiguraci jsou buď spravovány produktem IBM MQ, jako např. soubor `mqs.ini` na systémech AIX, Linux, and Windows , nebo součástí vaší vlastní správy konfigurací, jako např. konfiguračních skriptů **MQSC** . Zálohování a obnova pomocí archivu souborů.
- Výstup pro celou instalaci, například trasování, protokoly chyb a soubory FFDC. Soubory jsou uloženy v podadresářích `errors` a `trace` ve výchozím datovém adresáři. Výchozí datový adresář na systémech AIX and Linux je `/var/mqm`. V systému Windows je výchozím datovým adresářem instalační adresář IBM MQ .

Pomocí záložního správce front můžete také provádět pravidelné zálohy médií správce front s více instancemi s použitím lineárního protokolování. Záložní správce front neposkytuje obnovu, která je tak rychlá jako ze zrcadleného systému souborů, a neobnovuje změny od poslední zálohy. Mechanizmus záložního správce front je vhodnější pro použití ve scénářích zotavení z havárie mimo pracoviště než obnova správce front po lokalizovaném selhání úložiště.

Kombinace řešení dostupnosti IBM MQ

Aplikace používají jiné schopnosti produktu IBM MQ ke zlepšení dostupnosti. Správci front s více instancemi doplňují další funkce vysoké dostupnosti.

IBM MQ Klastry zvyšují dostupnost fronty

Dostupnost fronty můžete zvýšit vytvořením více definic fronty klastru; nejvýše jedné z každé fronty v každém správci v klastru.

Předpokládejme, že člen klastru selže a pak se do fronty klastru odešle nová zpráva. Pokud zpráva *nemá* přejít na správce front, který selhal, je zpráva odeslána jinému spuštěnému správci front v klastru, který má definici fronty.

Ačkoli klastry výrazně zvyšují dostupnost, existují dva související scénáře selhání, které vedou ke zpoždění zpráv. Sestavení klastru se správci front s více instancemi snižuje pravděpodobnost zpoždění zprávy.

Marooned zprávy

Dojde-li k selhání správce front v klastru, nebudou do správce front, který selhal, směrovány žádné další zprávy, které lze směrovat na jiné správce front v klastru. Zprávy, které již byly odeslány, jsou marokované, dokud není správce front, který selhal, restartován.

Afinity

Afinita je termín používaný k popisu informací sdílených mezi dvěma jinak samostatnými 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 jednotlivých zpráv v závislosti na předchozích zprávách.

Pokud posíláte zprávy do klastrovaných front, musíte zvážit afinitu. Potřebujete odeslat následné zprávy stejnému správci front, nebo může každá zpráva přejít na libovolného člena klastru?

Potřebujete-li odeslat zprávy stejnému správci front v klastru a dojde-li k selhání, budou zprávy čekat v přenosové frontě odesilatele, dokud nebude správce front klastru, který selhal, znovu spuštěn.

Je-li klastr konfigurován se správci front s více instancemi, je prodleva čekání na restartování správce front, u kterého došlo k selhání, omezena na dobu asi jedné minuty během převzetí pohotovostního režimu. Při spuštěném pohotovostním režimu se obnoví zpracování zónových zpráv, spustí se kanály pro nově aktivovanou instanci správce front a začnou proudit zprávy čekající v přenosových frontách.

Možným způsobem, jak nakonfigurovat klastr tak, aby překonal zpožděné zprávy správcem front, který selhal, je implementovat dva různé správce front na každý server v klastru a zajistit, aby jeden byl aktivní a jeden byl záložní instancí různých správců front. Jedná se o konfiguraci aktivního pohotovostního režimu, která zvyšuje dostupnost klastru.

Kromě výhod snížené administrace a zvýšené rozšiřitelnosti poskytují klastry další prvky dostupnosti, které doplňují správce front s více instancemi. Klastry chrání před jinými typy selhání, které ovlivňují aktivní i rezervní instance správce front.

Nepřerušená služba

Klastr poskytuje nepřerušenou službu. Nové zprávy přijaté klastrem jsou odeslány aktivním správcům front ke zpracování. Nespoléhejte na to, že správce front s více instancemi poskytne nepřerušenou službu, protože pohotovostnímu správci front trvá určitou dobu, než zjistí selhání a dokončí své spuštění, znovu připojí své kanály a znovu předloží nezdařené dávky zpráv.

Lokalizovaný výpadek

Existují praktická omezení, pokud jde o to, jak daleko od sebe mohou být aktivní, záložní a servery souborového systému, protože potřebují interagovat s milisekundovými rychlostmi, aby poskytovaly přijatelný výkon.

Klastrovaní správci front vyžadují rychlost interakce v řádu mnoha sekund a mohou být geograficky rozptýleni kdekoli na světě.

Provozní chyba

Použitím dvou různých mechanismů ke zvýšení dostupnosti snížíte pravděpodobnost, že provozní chyba, například lidská chyba, sníží vaše úsilí o dostupnost.

Skupiny sdílení front zvyšují dostupnost zpracování zpráv

z/OS Skupiny sdílení front poskytované pouze v systému z/OSumožňují skupině správců front sdílet obsluhující frontu. Pokud jeden správce front selže, ostatní správci front budou pokračovat ve

zpracování všech zpráv ve frontě. Správci front s více instancemi nejsou v produktu z/OS podporováni a doplňují skupiny sdílení front pouze jako součást širší architektury systému zpráv.

IBM MQ Klienti zvyšují dostupnost aplikací

Programy IBM MQ MQI client se mohou připojovat k různým správcům front ve skupině správců front na základě dostupnosti správce front, váhy připojení a afinit. Spuštěním aplikace v jiném počítači, než ve kterém je spuštěn správce front, můžete zlepšit celkovou dostupnost řešení, pokud existuje způsob, jak znovu připojit aplikaci, pokud dojde k selhání instance správce front, ke které je připojen.

Skupiny správců front se používají ke zvýšení dostupnosti klienta odpojením klienta od správce front, který je zastaven, a vyrovnáváním zátěže připojení klienta v rámci skupiny správců front, spíše jako sprejer IP. Klientská aplikace nesmí mít žádné afinity k nezdařenému správci front, například závislost na konkrétní frontě, nebo nemůže pokračovat ve zpracování.

Automatické opětovné připojení klienta a správci front s více instancemi zvyšují dostupnost klienta řešením některých problémů s afinitou. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Můžete nastavit volbu `MQCNO` `MQCNO_RECONNECT_Q_MGR`, chcete-li vynutit, aby se klient znovu připojil ke stejnému správci front:

1. Pokud dříve připojený správce front s jednou instancí není spuštěn, bude připojení zopakováno, dokud nebude správce front znovu spuštěn.
2. Je-li správce front konfigurován jako správce front s více instancemi, klient se znovu připojí k libovolné aktivní instanci.

Po automatickém opětovném připojení ke stejnému správci front se obnoví velká část informací o stavu, které správce front zadával jménem klienta, například fronty, které měl otevřené a téma, k němuž byl přihlášen k odběru. Pokud klient otevřel dynamickou frontu pro odpověď, aby obdržel odpověď na požadavek, obnoví se také připojení k frontě pro odpověď.

Linux MQ Adv. Vysoká dostupnost RDQM

RDQM (správce front replikovaných dat) je řešení vysoké dostupnosti, které je k dispozici na platformách Red Hat Enterprise Linux for x86-64 .

Konfigurace RDQM se skládá ze tří serverů nakonfigurovaných ve skupině s vysokou dostupností (HA), z nichž každý má instanci správce front. Jedna instance je spuštěný správce front, který synchronně replikuje svá data do dalších dvou instancí. Pokud server, na kterém je spuštěn tento správce front, selže, spustí se další instance správce front a bude mít aktuální data pro práci. Tři instance správce front mohou volitelně sdílet plovoucí adresu IP, takže klienti musí být konfigurováni pouze s jedinou adresou IP. V daném okamžiku může být spuštěna pouze jedna instance správce front, a to i v případě, že se skupina HA stane rozdělenou na oblasti kvůli problémům se sítí. Server, na kterém je spuštěn správce front, je označován jako 'primární', každý z ostatních dvou serverů je označován jako 'sekundární'.

Tři uzly se používají k výraznému snížení možnosti vzniku rozštěpené mozkové situace. Ve dvouuzlovém systému s vysokou dostupností může dojít k rozdělení mozku, když je přerušena konektivita mezi dvěma uzly. Bez konektivity mohou oba uzly spustit správce front současně a shromažďovat různá data. Při obnově připojení existují dvě různé verze dat ("rozštěpený mozek") a je nutný ruční zásah, aby se rozhodovalo, která datová sada se má uchovat a která se má vyřadit.

RDQM používá tříuzlový systém s kvorem, aby se vyhnul situaci rozděleného mozku. Uzly, které mohou komunikovat s alespoň jedním z ostatních uzlů, tvoří kvorum. Správci front mohou být spouštěny pouze v uzlu, který má kvorum. Správce front nemůže být spuštěn v uzlu, který není připojen alespoň k jednomu jinému uzlu, takže nemůže být spuštěn ve dvou uzlech současně:

- Dojde-li k selhání jednoho uzlu, může být správce front spuštěn na jednom z dalších dvou uzlů. Pokud dojde k selhání dvou uzlů, nelze správce front spustit na zbývajícím uzlu, protože uzel nemá kvorum (zbývající uzel nemůže určit, zda došlo k selhání ostatních dvou uzlů, nebo zda jsou stále spuštěny a ztratila konektivitu).

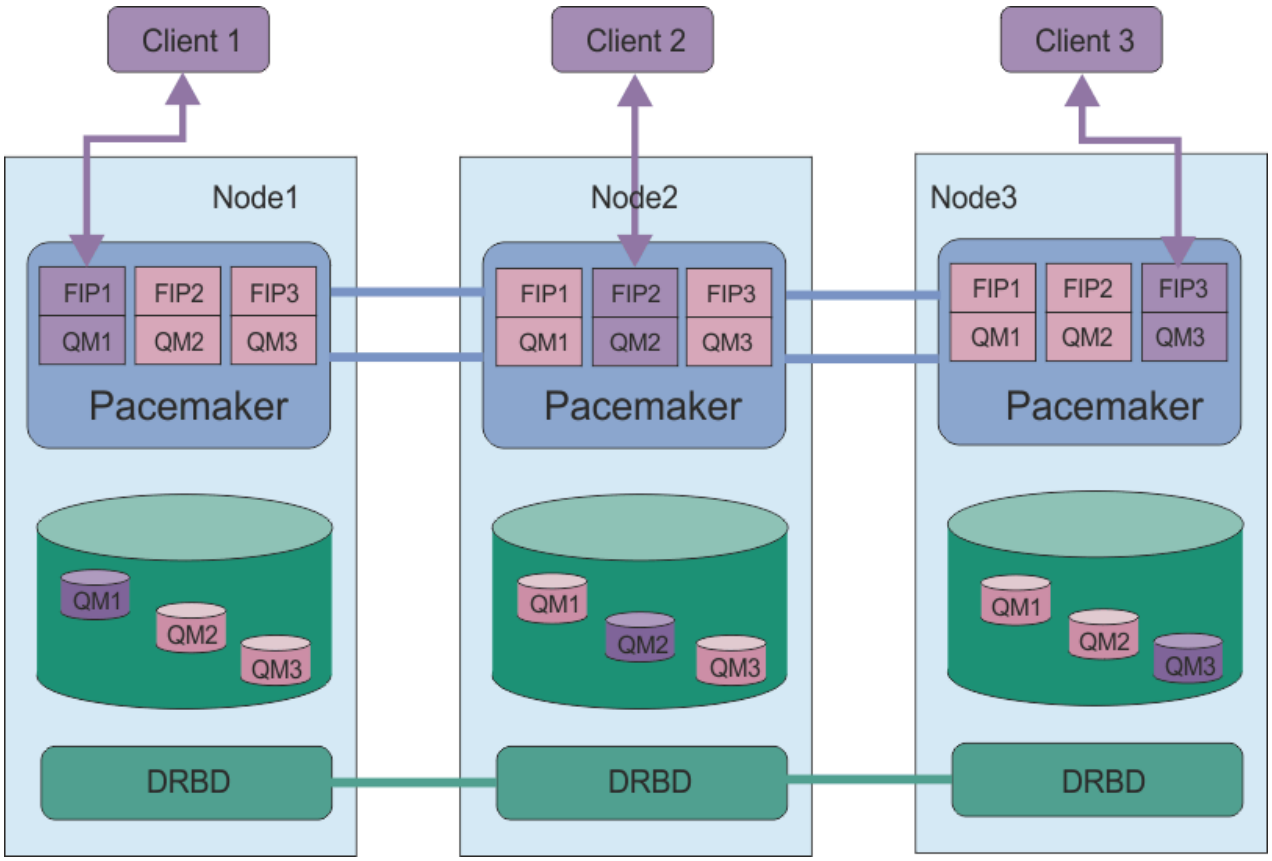
- Pokud jeden uzel ztratí konektivitu, nelze správce front v tomto uzlu spustit, protože uzel nemá kvorum. Správce front může být spuštěn na jednom ze zbývajících dvou uzlů, které mají kvorum. Pokud všechny uzly ztratí konektivitu, nelze správce front spustit na žádném z uzlů, protože žádný z uzlů nemá kvorum.

Poznámka: Agent IBM MQ Console nepodporuje správce front replikovaných dat. Produkt IBM MQ Explorer můžete použít se správci front replikovaných dat, ale nezobrazuje informace specifické pro funkce RDQM.

Konfigurace skupiny tří uzlů je zpracována produktem Pacemaker. Replikaci mezi těmito třemi uzly zpracovává DRBD. (Informace o modulu Pacemaker a https://docs.linbit.com/docs/users-guide-9.0/ informace o modulu DRBD naleznete v tématu https://clusterlabs.org/pacemaker/ .)

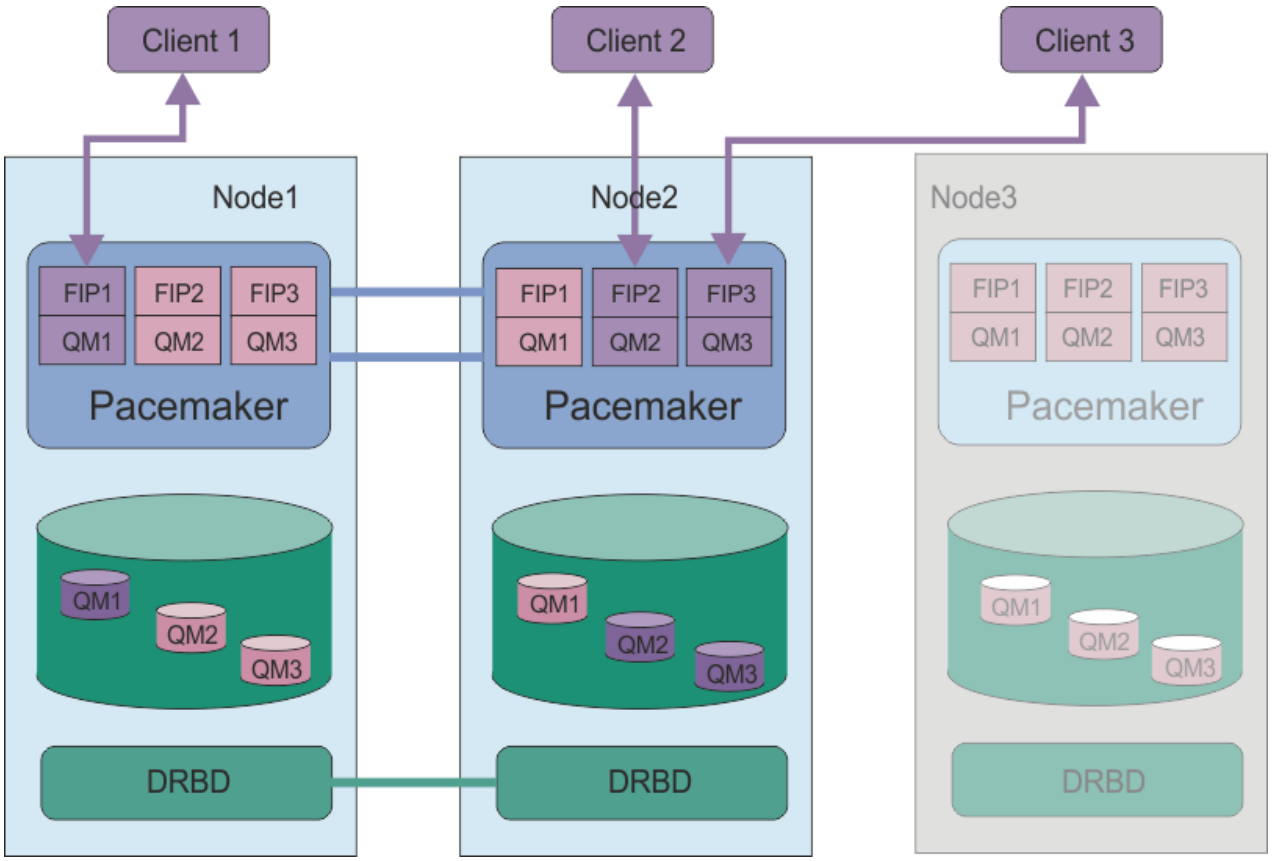
Správce front replikovaných dat můžete zálohovat pomocí procesu popsaného v tématu “Zálohování dat správce front” na stránce 651. Zastavení správce front a jeho zálohování nemá žádný vliv na monitorování uzlu prováděné konfigurací RDQM.

Následující obrázek ukazuje typickou implementaci s RDQM spuštěným na každém ze tří uzlů ve skupině HA.



Obrázek 78. Příklad skupiny HA se třemi RDQM

Na následujícím obrázku se uzel Node3 nezdařil, odkazy Pacemaker byly ztraceny a správce front QM3 je spuštěn na uzlu Node2 .



Obrázek 79. Příklad po selhání node3

Poznámka: Když správci front přejdou na jiný uzel, zachová si stav, který měli při překonání selhání. Spuštění správci front, kteří byli zastaveni, zůstanou zastaveni.

Související úlohy

Instalace RDQM (správci front replikovaných dat)

Použití aktualizací úrovně údržby pro RDQM

Migrace správců front replikovaných dat

Odstraňování problémů s konfiguracemi RDQM

Linux *Požadavky na řešení RDQM HA*

Před konfigurací skupiny RDQM s vysokou dostupností (HA) musíte splnit několik požadavků.

Systémové požadavky

Před konfigurací skupiny RDQM HA musíte dokončit nějakou konfiguraci na každém ze tří serverů, které mají být součástí skupiny HA.

- Každý uzel vyžaduje skupinu disků s názvem `drbdpool`. Úložiště pro každého správce front replikovaných dat je přiděleno jako samostatný logický svazek pro každého správce front z této skupiny disků. Pro dosažení nejlepšího výkonu by měla být tato skupina disků tvořena jedním nebo více fyzickými disky, které odpovídají interním diskovým jednotkám (nejlépe SSD). Produkt `drbdpool` můžete vytvořit před nebo po instalaci řešení RDQM HA, ale musíte vytvořit produkt `drbdpool` před tím, než skutečně vytvoříte jakékoli RDQM. Zkontrolujte konfiguraci skupiny disků pomocí příkazu **vgs** . Výstup by měl vypadat přibližně následovně:

```
  VG       #PV #LV #SN Attr   VSize   VFree
  drbdpool   1   9   0 wz--n- <16.00g <7.00g
  rhel       1   2   0 wz--n- <15.00g     0
```

Zejména zkontrolujte, zda v šestém sloupci atributů není znak c (tj. `wz--nc`). Hodnota c označuje, že je povoleno klastrování, a pokud je to, musíte odstranit skupinu disků a znovu ji vytvořit bez klastrování.

- Po vytvoření skupiny disků `drbdpool` s ní nic jiného neudělejte. Produkt IBM MQ spravuje logické disky vytvořené v produktu `drbdpool`a způsob a místo jejich připojení.
- Každý uzel vyžaduje až tři rozhraní, která se používají pro konfiguraci podpory RDQM:
  - Primární rozhraní pro Pacemaker pro monitorování skupiny HA.
  - Alternativní rozhraní pro Pacemaker pro monitorování skupiny HA.
  - Rozhraní pro synchronní replikaci dat, které je známé jako replikační rozhraní. To by mělo mít dostatečnou šířku pásma pro podporu požadavků replikace vzhledem k očekávané pracovní zátěži všech správců front replikovaných dat spuštěných ve skupině HA.

  Skupinu HA můžete nakonfigurovat tak, aby se pro všechna tři rozhraní používala stejná adresa IP, pro každé rozhraní se používá oddělená adresa IP nebo pro primární a alternativní a pro rozhraní replikace se používá stejná adresa IP.

  Pro maximální odolnost proti poruchám by měla být tato rozhraní nezávislá na kartách síťového rozhraní (NIC).
- DRBD vyžaduje, aby měl každý uzel ve skupině s vysokou dostupností platný název hostitele v síti Internet (hodnotu vrácenou produktem `uname -n`), jak definuje RFC 952 ve znění RFC 1123.
- Pokud mezi uzly ve skupině HA existuje brána firewall, musí brána firewall povolit provoz mezi uzly na řadě portů. Je poskytnut ukázkový skript `/opt/mqm/samp/rdqm/firewalld/configure.sh`, který otevře nezbytné porty, pokud spouštíte standardní bránu firewall v systému RHEL. Skript musíte spustit jako `root`. Používáte-li jinou bránu firewall, zkontrolujte definice služeb `/usr/lib/firewalld/services/rdqm*` a zjistěte, které porty je třeba otevřít. Skript přidá následující trvalá pravidla služby firewallD pro DRBD, Pacemakera IBM MQ:
  - MQ_INSTALLATION_PATH/samp/rdqm/firewalld/services/rdqm-drbd.xml umožňuje porty TCP 7000-7100.
  - MQ_INSTALLATION_PATH/samp/rdqm/firewalld/services/rdqm-pacemaker.xml umožňuje porty UDP 5404-5407
  - MQ_INSTALLATION_PATH/samp/rdqm/firewalld/services/rdqm-mq.xml umožňuje port TCP 1414 (skript musíte upravit, pokud požadujete jiný port)
- Pokud systém používá SELinux v režimu vynucení, možná budete muset spustit následující příkaz:

```
semanage permissive -a drbd_t
```

V 9.3.0.1 V 9.3.2 Pokud jste nainstalovali balík `drbd-selinux` , nemusíte spouštět **semanage**. Buď musíte mít tento balík nainstalovaný na každém uzlu, nebo musíte spustit **semanage** na každém uzlu.

Síťové požadavky

Doporučuje se vyhledat tři uzly ve skupině RDQM HA ve stejném datovém středisku.

Pokud se rozhodnete vyhledat uzly v různých datových střediscích, mějte na paměti následující omezení:

- Výkon rychle klesá se zvyšující se latencí mezi datovými středisky. Ačkoli produkt IBM bude podporovat latenci až 5 ms, můžete zjistit, že výkon aplikace nemůže tolerovat více než 1 až 2 ms latence.
- Data odeslaná přes odkaz replikace nepodléhají žádnému dalšímu šifrování kromě toho, které by mohlo být zavedeno z použití IBM MQ AMS.

Volitelně můžete nakonfigurovat plovoucí adresu IP tak, aby klient mohl používat stejnou adresu IP pro správce front replikovaných dat (RDQM) bez ohledu na to, na kterém uzlu ve skupině HA je spuštěn. Plovoucí adresa se váže na pojmenované fyzické rozhraní na primárním uzlu pro RDQM. Pokud dojde k selhání RDQM a jiný uzel se stane primárním uzlem, plovoucí adresa IP je svázána s rozhraním se stejným názvem na novém primárním uzlu. Fyzická rozhraní na třech uzlech musí mít stejný název a musí patřit do stejné podsítě jako plovoucí adresa IP.

Požadavky uživatele na konfiguraci klastru

Skupinu RDQM HA můžete nakonfigurovat jako uživatele `root`. Nechcete-li konfigurovat jako `root`, konfigurujte místo toho uživatele ve skupině `mqm` . Aby mohl uživatel ve skupině `mqm` konfigurovat klastr RDQM, musí splňovat následující požadavky:

- Uživatel `mqm` musí být schopen použít příkaz sudo ke spuštění příkazů na každém ze tří serverů, které tvoří skupinu RDQM HA.
- Pokud může uživatel `mqm` použít SSH bez hesla ke spuštění příkazů na každém ze tří serverů, které tvoří skupinu RDQM HA, pak musí spustit příkazy pouze na jednom ze serverů.
- Uživatel `mqm` musí mít na všech třech serverech stejné UID.
- Skupina `mqm` musí mít stejné GID na všech třech serverech.

Příkaz sudo musíte nakonfigurovat tak, aby uživatel `mqm` mohl spouštět následující příkazy s oprávněním uživatele root:

```
/opt/mqm/bin/crtmqm
/opt/mqm/bin/dltmqm
/opt/mqm/bin/rdqmadm
/opt/mqm/bin/rdqmstatus
```

Uživatelské požadavky pro práci se správci front

Chcete-li vytvořit, odstranit nebo konfigurovat správce front replikovaných dat (RDQMs), musíte použít ID uživatele, které patří do skupin `mqm` i `haclient` (skupina `haclient` je vytvořena během instalace komponenty Pacemaker).

Linux *Nastavení zabezpečení SSH bez hesla*

Můžete nastavit zabezpečení SSH bez hesla, takže budete potřebovat zadat pouze konfigurační příkazy na jednom uzlu ve skupině HA. (Nastavení zabezpečení SSH bez hesla je volitelné, případně můžete příkazy ručně zkopírovat do každého uzlu.)

Informace o této úloze

Chcete-li nastavit zabezpečení SSH bez hesla, musíte nakonfigurovat ID `mqm` na každém uzlu, pak vygenerujte klíč na každém uzlu pro tohoto uživatele. Poté distribuujete klíče do ostatních uzlů a otestujete připojení, abyste přidali každý uzel do seznamu známých hostitelů. Nakonec zamknete ID `mqm` .

Poznámka: Pokyny předpokládají, že definujete skupinu HA s oddělenými primárními, alternativními a replikačními rozhraními, a proto definujete přístup SSH bez hesla přes primární a alternativní rozhraní. Pokud plánujete nakonfigurovat systém s jedinou adresou IP, pak nadefinujete přístup SSH bez hesla přes toto jediné rozhraní.

RDQM vyžaduje, aby příkaz `ssh` fungoval bez interakce, tj. bez výzvy k zadání hesla atd.

Postup

1. Na každém ze tří uzlů postupujte takto, chcete-li nastavit uživatele `mqm` a vygenerovat klíč SSH:
   a) Změňte domovský adresář `mqm` na `/home/mqm`:

   ```
   usermod -d /home/mqm mqm
   ```

   b) Vytvořte adresář `/home/mqm` :

   ```
   mkhomedir_helper mqm
   ```

   c) Přidejte heslo `mqm` :

   ```
   passwd mqm
   ```

d) Spusťte interaktivní shell jako mqm:

```
su mqm
```

e) Vygenerujte ověřovací klíč mqm :

```
ssh-keygen -t rsa -f /home/mqm/.ssh/id_rsa -N ''
```

2. Na každém ze tří uzlů přidejte klíč tohoto uzlu do ostatních dvou uzlů a otestujte připojení pro každý primární uzel a (pokud se používá) alternativní adresy:

a) Přidat klíč ke vzdáleným uzlům

```
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node1_primary_address
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node1_alternate_address
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node2_primary_address
ssh-copy-id -i /home/mqm/.ssh/id_rsa.pub remote_node2_alternate_address
```

b) Zkontrolujte ssh bez hesla a aktualizujte known_hosts pro vzdálené uzly:

```
ssh remote_node1_primary_address uname -n
ssh remote_node1_alternate_address uname -n
ssh remote_node2_primary_address uname -n
ssh remote_node2_alternate_address uname -n
```

Pro každé připojení budete vyzváni k potvrzení, že chcete pokračovat. Potvrďte pro každý z nich aktualizovat known_hosts. Musíte to dokončit, než se pokusíte nakonfigurovat skupinu HA pomocí zabezpečení SSH bez hesla.

c) Ukončete interaktivní shell jako mqm:

```
exit
```

3. Na každém uzlu, jako uživatel root, postupujte takto, chcete-li odebrat heslo mqm a zamknout ID:

a) Odeberte heslo mqm :

```
passwd -d mqm
```

b) Zamknout mqm:

```
passwd -l mqm
```

4. V každém uzlu, jako uživatel root, postupujte takto, chcete-li nastavit přístup k příkazu sudo pro uživatele mqm :

a) Upravte soubor sudoers pomocí příkazu **visudo** :

```
visudo
```

b) Vyhledejte řádek "*## Allows people in group wheel to run all commands*" a přidejte pod něj následující text:

```
#%mqm    ALL=(ALL)       ALL
```

c) Vyhledejte řádek "*## Same thing without a password*" a přidejte pod něj následující text:

```
%mqm            ALL=(ALL)       NOPASSWD: ALL
```

Linux *Definování klastru Pacemaker (skupina HA)*

Skupina HA je klastr Pacemaker . Klastr Pacemaker definujete tak, že upravíte soubor /var/mqm/rdqm.ini a spustíte příkaz **rdqmadm** .

Informace o této úloze

Informace o modulu Pacemakernaleznete v části https://clusterlabs.org/pacemaker/ . Klastr Pacemaker můžete vytvořit jako uživatel ve skupině `mqm` , pokud může uživatel `mqm` používat `sudo`. Pokud může uživatel také SSH na každém serveru bez hesla, stačí upravit soubor `rdqm.ini` a spustit **`rdqmadm`** na jednom ze serverů pro vytvoření klastru Pacemaker . Jinak musíte vytvořit soubor a spustit příkaz jako `root` na každém ze serverů, které mají být uzly.

Soubor `rdqm.ini` poskytuje adresy IP, které používá RDQM pro uzly v klastru Pacemaker . Pro instalace RHEL 8 a RHEL 9 musíte zadat název každého uzlu, který musí být názvem hostitele vráceným příkazem **`uname -n`** . Pro instalace RHEL 7 je specifikace názvu uzlu nepovinná.

Skupinu RDQM HA lze nakonfigurovat tak, aby používala jednu, dvě nebo tři adresy IP:

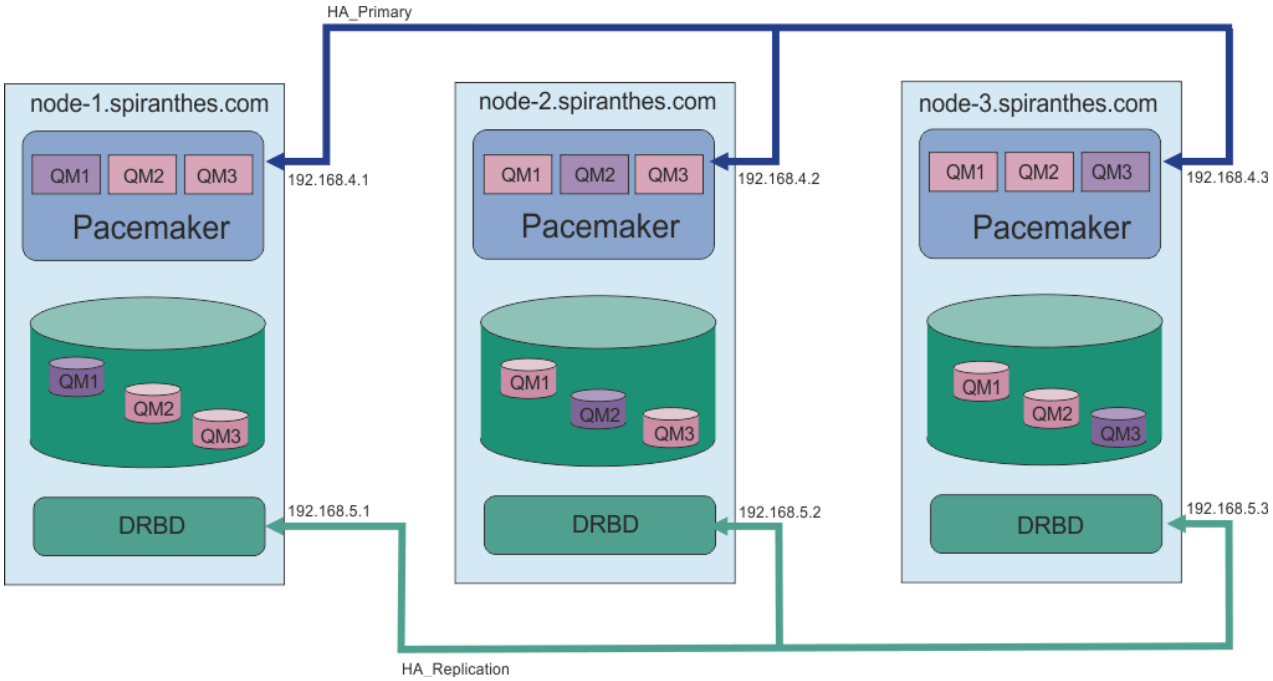
- Jedna IP adresa: Heartbeats a replikace sdílejí stejný odkaz
- Dvě adresy IP: Heartbeats a replikace používají samostatné odkazy
- Tři adresy IP: Jeden odkaz pro replikaci a dva samostatné odkazy pro prezenční signály.

Tyto volby jsou k dispozici pro podporu různých šablon implementace pro RDQM. Různé volby lze použít k maximalizaci odolnosti řešení RDQM na základě použitého prostředí. Konfigurace, které používají buď dvě, nebo tři adresy IP, jsou primárně určeny pro implementace, kde je vyžadováno podrobné řízení toho, která fyzická síť spojuje prezenční signály a replikační provoz, aby nakonfigurovala redundanci pro konektivitu mezi uzly. Alternativně lze vysoce dostupnou a odolnou konektivitu implementovat na síťové vrstvě, například pomocí agregace linek. Při agregaci linek se používá více fyzických síťových propojení k poskytnutí jednoho logického propojení, které může i nadále fungovat, pokud jednotlivá fyzická propojení selžou. Pokud je RDQM implementován v prostředí, kde je síťová konektivita virtualizována a/nebo kde je na síťové vrstvě implementována odolná konektivita, pak je obvykle vhodnější použít jedinou adresu IP pro prezenční signály i replikaci.

Následující příklad ilustruje použití dvou adres IP. Váš soubor `rdqm.ini` má pole `HA_Primary` a `HA_Replication` pro každý uzel, ale žádné pole `HA_Alternate` :

```
Node:
  Name=rdqm-node-1.spiranthes.com
  HA_Primary=192.168.4.1
  HA_Replication=192.168.5.1
Node:
  Name=rdqm-node-2.spiranthes.com
  HA_Primary=192.168.4.2
  HA_Replication=192.168.5.2
Node:
  Name=rdqm-node-3.spiranthes.com
  HA_Primary=192.168.4.3
  HA_Replication=192.168.5.3
```

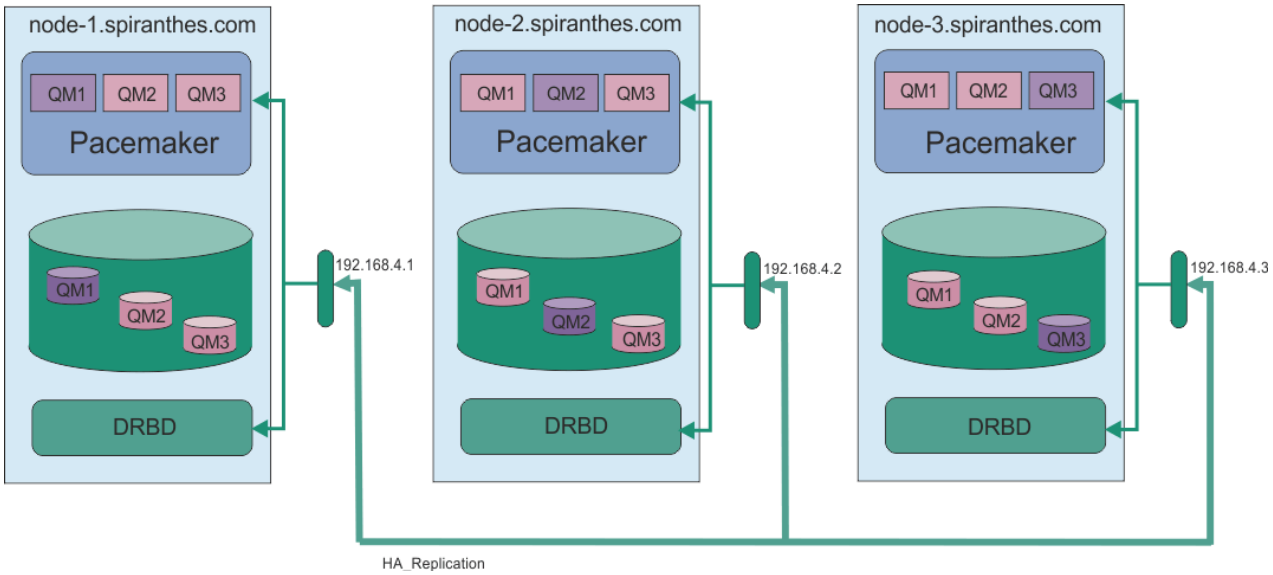
Tuto konfiguraci ilustruje následující diagram:



Následující ukázkový soubor zobrazuje konfiguraci pro příklad klastru Pacemaker , který používá rozhraní `HA_Replication` pro monitorování (například lze použít pro implementaci ověření koncepce). V tomto případě zadáváte pouze rozhraní `HA_Replication` :

```
Node:
  Name=rdqm-node-1.spiranthes.com
  HA_Replication=192.168.4.1
Node:
  Name=rdqm-node-2.spiranthes.com
  HA_Replication=192.168.4.2
Node:
  Name=rdqm-node-3.spiranthes.com
  HA_Replication=192.168.4.3
```

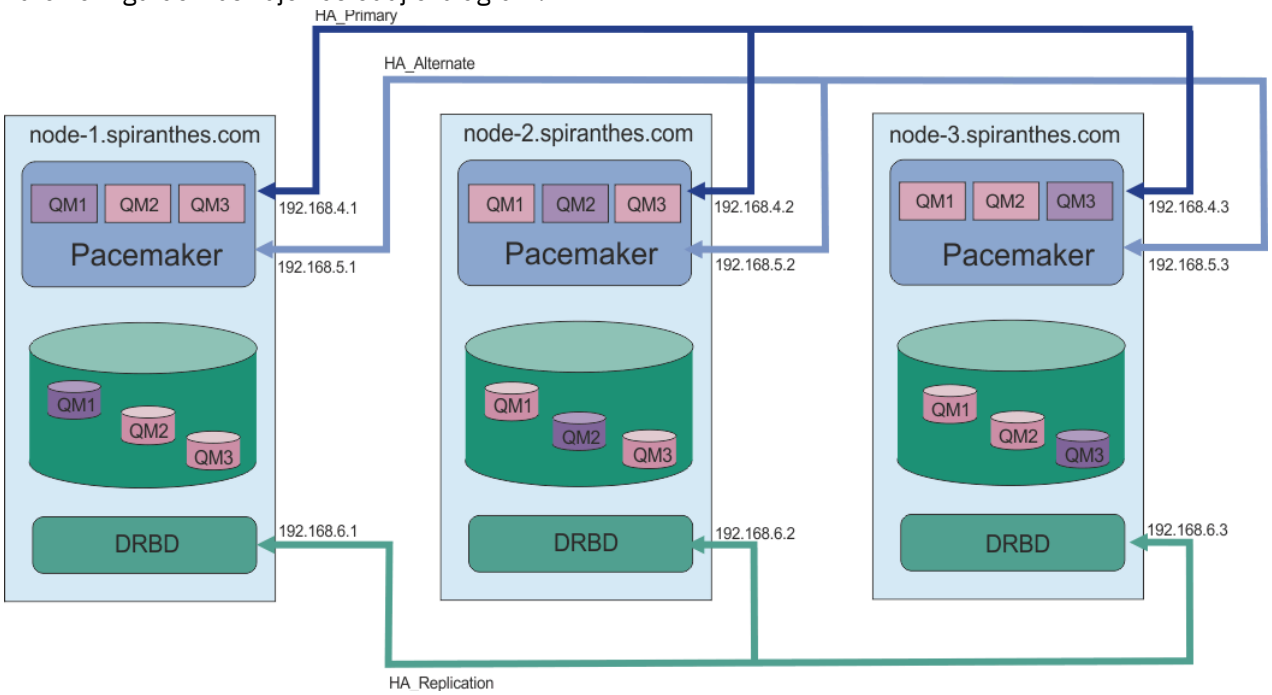
Tuto konfiguraci ilustruje následující diagram:



Následující ukázkový soubor zobrazuje konfiguraci pro příklad klastru Pacemaker , který používá oddělenou adresu IP pro každé rozhraní:

```
Node:
  Name=rdqm-node-1.spiranthes.com
  HA_Primary=192.168.4.1
  HA_Alternate=192.168.5.1
  HA_Replication=192.168.6.1
Node:
  Name=rdqm-node-2.spiranthes.com
  HA_Primary=192.168.4.2
  HA_Alternate=192.168.5.2
  HA_Replication=192.168.6.2
Node:
  Name=rdqm-node-3.spiranthes.com
  HA_Primary=192.168.4.3
  HA_Alternate=192.168.5.3
  HA_Replication=192.168.6.3
```

Tuto konfiguraci ilustruje následující diagram:



Pořadí, ve kterém uvedete uzly, musí být stejné ve všech souborech `rdqm.ini` ve vaší konfiguraci. Vaše tři uzly musí mít společný pohled na to, který z nich je Node1, který Node2 atd.

Procedura

- Chcete-li definovat klastr Pacemaker jako uživatel `root`, postupujte takto:
  a) Upravte soubor `/var/mqm/rdqm.ini` na jednom ze tří serverů tak, aby tento soubor definoval klastr.
  b) Zkopírujte soubor na další dva servery, které budou uzly v klastru Pacemaker .
  c) Spusťte následující příkaz jako `root` na každém ze tří serverů:

  ```
  rdqmadm -c
  ```

- Chcete-li definovat klastr Pacemaker jako uživatele ve skupině `mqm` na každém uzlu, postupujte takto:
  a) Ujistěte se, že uživatel `mqm` může použít **sudo** ke spuštění příkazů.
  b) Upravte soubor `/var/mqm/rdqm.ini` na jednom ze tří serverů tak, aby soubor definoval klastr Pacemaker .
  c) Zkopírujte soubor `/var/mqm/rdqm.ini` na další dva servery, které budou uzly v klastru Pacemaker .

d) Na každém serveru spusťte následující příkaz:

```
rdqmadm -c
```

- Chcete-li definovat klastr Pacemaker jako uživatele ve skupině `mqm` z jednoho uzlu, postupujte takto:
  a) Ujistěte se, že uživatel `mqm` může použít **sudo** ke spuštění příkazů a může se připojit ke každému serveru pomocí SSH bez hesla.
  b) Upravte soubor `/var/mqm/rdqm.ini` na jednom ze tří serverů tak, aby soubor definoval klastr Pacemaker .
  c) Spusťte následující příkaz:

```
rdqmadm -c
```

Související odkazy
rdqmadm (spravovat klastr správce front replikovaných dat)

Linux *Odstranění klastru Pacemaker (skupina HA)*
Skupina HA je klastr Pacemaker . Konfiguraci klastru Pacemaker můžete odstranit spuštěním příkazu **rdqmadm** s volbou `-u` .

Informace o této úloze

Konfiguraci klastru Pacemaker nelze odstranit, pokud na některém z uzlů stále existují žádní správci front replikovaných dat.

Procedura

- Chcete-li odstranit konfiguraci klastru Pacemaker , zadejte z libovolného uzlu následující příkaz:

```
rdqmadm -u
```

Související odkazy
rdqmadm (spravovat klastr správce front replikovaných dat)

Linux ***Vytvoření HA RDQM***
Příkaz **crtmqm** se používá k vytvoření správce front replikovaných dat s vysokou dostupností (RDQM).

Informace o této úloze

Můžete vytvořit správce front replikovaných dat s vysokou dostupností (RDQM) jako uživatele ve skupině `mqm` , pokud může uživatel mqm použít příkaz sudo. Pokud může uživatel také SSH na každém uzlu bez hesla, pak stačí spustit příkaz vytvoření RDQM na jednom uzlu a vytvořit RDQM na všech třech uzlech. Jinak musíte mít hodnotu `root` , abyste mohli vytvořit RDQM, a musíte spustit příkazy na všech třech uzlech.

Poznámka: Ve skupině s vysokou dostupností je absolutní limit 129 správců front. Pokusíte-li se vytvořit více než toto, pokus se nezdaří. V praxi může při přidávání více než 50 správců front do skupiny s vysokou dostupností dojít k problémům s časovým limitem.

Následující body poskytují určité vodítko při určování velikosti systému souborů správce front:

1. Při vytváření správce front RDQM je systém souborů přidělen k ukládání dat a protokolů správce front. Je důležité tento systém souborů vhodně nastavit tak, aby mohl správce front zaznamenávat probíhající aktivity do protokolů a ukládat zprávy aplikací do front. Při určování velikosti systému souborů zvažte požadavky na špičkový systém zpráv, budoucí růst pracovní zátěže a výpadky aplikací, které by mohly způsobit sestavení zpráv ve frontách. Informace o výpočtu velikosti protokolu pro zotavení správce front naleznete v části “Jak velký by měl být souborový systém protokolu?” na stránce 632. Při výpočtu požadavků na úložiště pro zprávy aplikace je třeba vzít v úvahu velikost a počet zpráv plus jejich záhlaví MQMD a všechny vlastnosti zpráv, které mají.

2. Velikost systémů souborů správce front RDQM nelze dynamicky měnit. Je-li to vyžadováno, je třeba provést zálohu a poté obnovit správce front RDQM s větším systémem souborů, viz "Změna velikosti systému souborů pro správce front HA RDQM" na stránce 563.
3. Velikost jednotlivých front na disku můžete omezit pomocí atributů lokální fronty, například MAXDEPTH a MAXFSIZE. Viz Úprava IBM MQ.
4. Měli byste monitorovat probíhající využití disku a odpovídajícím způsobem reagovat, pokud se využití disku zvýší dříve, než se využití systému souborů stane kritickým. Využití systému souborů lze monitorovat buď pomocí schopností platformy/operačního systému, nebo přihlášením k odběru metrik publikovaných v tématech systému IBM MQ , která jsou popsána v tématu Metriky publikované v tématech systému.

Procedura

- Chcete-li vytvořit RDQM jako uživatele ve skupině `mqm` , postupujte takto:
  a) Ujistěte se, že uživatel `mqm` může použít **sudo** ke spuštění příkazů a může se připojit ke každému serveru pomocí SSH bez hesla.
  b) Zadejte následující příkaz:

  ```
  crtmqm -sx [-fs FilesystemSize] qmname
  ```

  kde *qmname* je název správce front replikovaných dat. Volitelně můžete určit velikost systému souborů pro správce front (tj. velikost logického disku vytvořeného ve skupině disků drbdpool).

  Příkaz se pokusí použít SSH pro připojení k ostatním uzlům v klastru jako uživatel `mqm` . Pokud je připojení úspěšné, sekundární instance správce front se vytvoří na uzlech. Jinak musíte vytvořit sekundární instance a poté spustit příkaz **`crtmqm -sx`** (jak je popsáno pro uživatele `root`).
- Chcete-li vytvořit RDQM jako uživatel `root`:
  a) Zadejte následující příkaz na každém z uzlů, které mají být hostiteli sekundárních instancí RDQM:

  ```
  crtmqm -sxs [-fs FilesystemSize] qmname
  ```

  kde *qmname* je název správce front replikovaných dat. Volitelně můžete určit velikost systému souborů pro správce front (tj. velikost logického disku vytvořeného ve skupině disků drbdpool). Musíte uvést stejnou velikost systému souborů pro RDQM na všech třech uzlech ve skupině HA. Velikost je číselná hodnota uvedená v GB. Hodnotu v MB můžete zadat zadáním hodnoty následované znakem `M` .

  Příkaz vytvoří sekundární instanci RDQM.
  b) Ve zbývajícím uzlu zadejte následující příkaz:

  ```
  crtmqm -sx [-fs FilesystemSize] qmname
  ```

  kde *qmname* je název správce front replikovaných dat. Volitelně můžete určit velikost systému souborů pro správce front. Velikost je číselná hodnota uvedená v GB. Hodnotu v MB můžete zadat zadáním hodnoty následované znakem `M`.

  Příkaz určí, zda sekundární instance správce front existuje v ostatních dvou uzlech. Pokud existují sekundární soubory, příkaz vytvoří a spustí primárního správce front. Pokud sekundární uzly neexistují, budete vyzváni ke spuštění příkazu **`crtmqm -sxs`** na každém z uzlů.

  Kromě argumentů DataPath (**`-md`**) a LogPath (**`-ld`**) jsou všechny argumenty platné pro vytvoření standardního správce front Linux platné také pro primárního správce front replikovaných dat.

  Poznámka: Když vytvoříte RDQM, bude pro odkaz replikace přiděleno další volné číslo portu nad 7000. Pokud se zjistí, že zvolený port používá jiná aplikace, příkaz **`crtmqm`** selže s chybou AMQ6543 a tento port se přidá do seznamu vyloučení. Musíte odstranit sekundární instance správce front a poté znovu spustit příkaz **`crtmqm`** .

Související odkazy

crtmqm

Linux *Odstranění RDQM s vysokou dostupností*

Pomocí příkazu **dltmqm** můžete odstranit správce front replikovaných dat s vysokou dostupností (RDQM).

Informace o této úloze

Musíte spustit příkaz k odstranění RDQM na primárním uzlu RDQM. Nejprve musí být ukončen RDQM. Příkaz můžete spustit jako uživatel mqm, pokud má tento uživatel nezbytná oprávnění k příkazu sudo. Jinak musíte příkaz spustit jako uživatel root. Po odstranění prostředků přidružených k primárnímu správci front se příkaz pokusí odstranit sekundární správce front pomocí ssh pro připojení k ostatním uzlům. Pokud se toto odstranění nezdaří, musíte spustit `dltmqm` ručně na ostatních uzlech, abyste dokončili proces. V sekundárním uzlu příkaz selže, pokud ještě nebyl odstraněn primární správce front.

Procedura

- Chcete-li odstranit RDQM, zadejte následující příkaz:

```
dltmqm RDQM_name
```

Související odkazy

dltmqm

Linux MQ Adv. *Migrace správce front na správce front HA RDQM*

Existujícího správce front můžete migrovat tak, aby se stal správcem front replikovaných dat s vysokou dostupností (RDQM), a to tak, že zálohujete jeho trvalá data a poté data obnovíte do nově vytvořeného správce front RDQM se stejným názvem.

Informace o této úloze

Správci front replikovaných dat HA vyžadují vyhrazený logický svazek (systém souborů) a konfiguraci replikace disku a řízení HA. Tyto komponenty jsou konfigurovány pouze při vytvoření nového správce front. Existujícího správce front lze migrovat pro použití RDQM zálohováním jeho trvalých dat a následným obnovením dat do nově vytvořeného správce front RDQM se stejným názvem. Tento postup zachovává konfiguraci, stav a trvalé zprávy správce front v době vytvoření zálohy.

Poznámka: Správce front lze migrovat pouze z verze produktu IBM MQ , která je stejná nebo nižší než verze, ve které je nainstalován produkt RDQM. Operační systém a architektura musí být stejné. Jinak musíte na cílové platformě vytvořit nového správce front. Viz téma Přesunutí správce front do jiného operačního systému.

Před migrací správce front byste měli splňovat následující podmínky:

- Vyhodnoťte požadavky na vysokou dostupnost a prohlédněte si téma “Vysoká dostupnost RDQM” na stránce 549.
- Zkontrolujte aplikace a správce front, kteří se připojují ke správci front. Zvažte změny nezbytné pro směrování připojení do uzlu RDQM, kde je spuštěn správce front. Pokud například konfigurujete vysokou dostupnost RDQM, můžete zvážit použití plovoucí adresy IP, viz “Vytvoření a odstranění plovoucí adresy IP” na stránce 566.
- Zajistěte nebo identifikujte existující uzly RDQM pro zvolenou konfiguraci. Informace o systémových požadavcích RDQM viz “Požadavky na řešení RDQM HA” na stránce 551.
- Nainstalujte produkt IBM MQ Advanced, který zahrnuje funkci RDQM, na každý uzel.
- Nakonfigurujte konfiguraci skupiny RDQM HA, viz “Definování klastru Pacemaker (skupina HA)” na stránce 554.
- Volitelně ověřte konfiguraci RDQM pomocí správce front testu, který lze poté odstranit. Testování konfigurace se doporučuje k identifikaci a vyřešení případných problémů před migrací správce front.
- Zkontrolujte konfiguraci zabezpečení pro správce front a poté proveďte replikaci požadovaných lokálních uživatelů a skupin v jednotlivých uzlech RDQM.

- Zkontrolujte konfiguraci správce front a kanálu a určete, zda jsou použity uživatelské procedury rozhraní API, uživatelské procedury kanálu nebo uživatelské procedury pro převod dat. Nainstalujte požadované uživatelské procedury na každý uzel RDQM.
- Zkontrolujte všechny definované služby správce front a poté nainstalujte a nakonfigurujte požadované procesy v každém uzlu RDQM.

Postup

1. Zazálohujte existujícího správce front:
   a) Zastavte existujícího správce front zadáním příkazu wait shutdown `endmqm -w`nebo příkazu immediate shutdown `endmqm -i`. Tento krok je důležitý pro zajištění konzistence dat v záloze.
   b) Určete umístění datového adresáře správce front zobrazením konfiguračního souboru IBM MQ `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`viz “IBM MQ konfigurační soubor mqs.ini” na stránce 85.

      Vyhledejte sekci `QueueManager` pro správce front v souboru. Pokud sekce obsahuje klíč s názvem `DataPath` , její hodnota je datový adresář správce front. Pokud klíč neexistuje, lze datový adresář správce front určit pomocí hodnot klíčů `Prefix` a `Directory` . Datový adresář správce front je zřetězením těchto hodnot ve tvaru *předpona*/qmgrs/*adresář*. Další informace o sekci QueueManager naleznete v části “QueueManager sekce souboru mqs.ini” na stránce 95.
   c) Vytvořte zálohu datového adresáře správce front. V systému Linuxto můžete provést pomocí příkazu **`tar`** . Chcete-li například zálohovat datový adresář pro správce front, můžete použít následující příkaz. Všimněte si posledního parametru příkazu, kterým je jedna tečka (tečka):

      ```
      tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
      ```

   d) Určete umístění adresáře protokolu správce front zobrazením IBM MQ konfiguračního souboru správce front `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front, qm.ini” na stránce 97.

      Adresář protokolu správce front je definován jako hodnota klíče `LogPath` v sekci `Log` . Informace o sekci viz “Sekce protokolu souboru qm.ini” na stránce 130.
   e) Vytvořte zálohu adresáře protokolu správce front. V systému Linuxto můžete provést pomocí příkazu tar. Chcete-li například zálohovat adresář protokolu pro správce front, můžete použít následující příkaz. Všimněte si posledního parametru příkazu, kterým je jedna tečka (tečka):

      ```
      tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
      ```

   f) Vytvořte zálohu všech úložišť certifikátů používaných správcem front, pokud nejsou umístěna v datovém adresáři správce front. Ujistěte se, že je zálohován soubor databáze klíčů i soubor pro uložení hesla. Informace o úložišti klíčů správce front naleznete v tématu Úložiště klíčů SSL/TLS a Vyhledání úložiště klíčů pro správce front. Informace o vyhledání úložiště klíčů AMS v případě, že je správce front konfigurován pro použití zachycení agenta MCA (AMS Message Channel Agent), naleznete v tématu Zachycení agenta MCA (Message Channel Agent).
   g) Existující správce front již není vyžadován, takže jej lze odstranit. Pokud je to však možné, měli byste odstranit existujícího správce front pouze po jeho úspěšném obnovení v cílovém systému. Odložení odstranění zajistí, že správce front bude možné restartovat, pokud se proces migrace nedokončí úspěšně.

      Poznámka: Pokud odložíte odstranění existujícího správce front, nerestartujte jej. Je důležité, aby správce front zůstal ukončen, protože během migrace dojde ke ztrátě dalších změn jeho konfigurace nebo stavu.
2. Připravte primární uzel RDQM:
   a) Vytvořte nového správce front RDQM se stejným názvem jako zálohovaný správce front. Ujistěte se, že systém souborů přidělený pro správce front RDQM produktem **`crtmqm`** je dostatečně velký na to, aby obsahoval data, primární protokoly a sekundární protokoly pro existujícího správce front, plus

další prostor pro budoucí rozšíření. Informace o vytvoření správce front RDQM viz "Vytvoření HA RDQM" na stránce 558.

b) Určete primární uzel RDQM pro správce front. Informace o tom, jak určit primární uzel, viz rdqmstatus (zobrazení stavu RDQM).

c) Pokud je v primárním uzlu RDQM spuštěn správce front RDQM, zastavte jej pomocí příkazu `endmqm -w` nebo `endmqm -i` .

d) V primárním uzlu RDQM určete umístění adresářů dat a protokolů pro správce front RDQM (použijte metody popsané v krocích 1b a 1d).

e) V primárním uzlu RDQM odstraňte obsah dat a adresářů protokolu správce front RDQM, nikoli však samotné adresáře.

3. Obnovte správce front v primárním uzlu RDQM:

a) Zkopírujte zálohy dat a adresářů protokolů správce front do primárního uzlu RDQM a dále všechny samostatné zálohy úložišť certifikátů používaných správcem front.

b) Obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a zajistěte zachování vlastnictví souborů a oprávnění. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1c , uživatel root může k její obnově použít následující příkaz:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

c) Obnovte zálohu adresáře protokolu správce front do prázdného adresáře protokolu pro nového správce front RDQM, čímž zajistíte zachování vlastnictví souboru a oprávnění. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1e , uživatel root může k její obnově použít následující příkaz:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

d) Upravte obnovený konfigurační soubor správce front `qm.ini`v datovém adresáři pro správce front RDQM. Aktualizujte hodnotu klíče `LogPath` v sekci `Log` tak, aby uváděla adresář protokolu pro správce front RDQM.

Přezkoumejte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Můžete například potřebovat aktualizovat následující cesty:

- Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
- Cesta pro uživatelské procedury, které jsou vyžadovány správcem front.
- Cesta k souborům načtení přepínače, pokud je správcem front koordinátor transakcí XA.

e) Je-li správce front konfigurován tak, aby používal zachytávání agenta MCA (AMS Message Channel Agent), zkopírujte úložiště klíčů AMS do nové instalace RDQM a poté zkontrolujte a aktualizujte konfiguraci. Úložiště klíčů musí být k dispozici v každém uzlu RDQM, takže pokud není umístěno v replikovaném systému souborů pro správce front, musí být zkopírováno do každého uzlu. Další informace naleznete v tématu Zachycení agenta MCA (Message Channel Agent).

f) Ověřte, že je správce front zobrazen příkazem **dspmq** a jeho stav je ohlášen jako ukončený. Následující příklad ukazuje ukázkový výstup pro správce front RDQM HA:

```
$ dspmq -o status -o ha

QMNAME(QM1) STATUS(Ended normally) HA(Replicated)
```

g) Pomocí příkazu **rdqmstatus** ověřte, zda byla obnovená data správce front replikována do sekundárních uzlů RDQM, a zobrazte tak stav správce front. Stav HA by měl být nahlášen jako `Normal` na každém uzlu. Následující příklad ukazuje ukázkový výstup pro správce front RDQM HA:

```
$ rdqmstatus -m QM1
Node:                           mqhavm10-adm
Queue manager status:           Ended normally
Queue manager file system:      50MB used, 0.2GB allocated [42%]
HA role:                        Primary
HA status:                      Normal
```

```
HA control:                     Disabled
HA current location:            This node
HA preferred location:          This node
HA floating IP interface:       None
HA floating IP address:         None

Node:                           mqhavm11-adm
HA status:                      Normal

Node:                           mqhavm12-adm
HA status:                      Normal
```

h) Spusťte správce front v primárním uzlu RDQM.

i) Připojte se ke správci front a aktualizujte hodnotu atributu správce front SSLKEYR tak, aby určovala nové umístění úložiště certifikátů správce front. Standardně je hodnota tohoto atributu nastavena na *queue_manager_data_directory*/ssl/key. Úložiště certifikátů musí být umístěno ve stejném umístění na každém uzlu RDQM. Pokud se úložiště nenachází v replikovaném systému souborů pro správce front, musí být zkopírováno do každého uzlu.

j) Zkontrolujte definice objektů IBM MQ pro správce front a aktualizujte hodnotu atributů objektů, které odkazují na změněná nastavení sítě, instalační adresář produktu IBM MQ nebo datový adresář správce front, včetně následujících objektů:

- Lokální adresy IP používané listenery (atributIPADDR).
- Lokální adresy IP používané kanály (atributLOCLADDR).
- Lokální adresy IP definované pro přijímací kanály klastru (atributCONNAME).
- Lokální adresy IP definované pro objekty informací o komunikaci (atributGRPADDR).
- Systémové cesty definované pro definice objektů procesů a služeb.

k) Zastavte a restartujte správce front, aby se změny projevily.

l) Zopakujte krok 3j pro vzdálené správce front a ekvivalentní nastavení pro aplikace, které se připojují k migrovanému správci front, včetně:

- Názvy připojení kanálu (atributCONNAME).
- Pravidla ověřování kanálu, která omezují příchozí připojení ze správce front na základě adresy IP nebo názvu hostitele.
- Tabulky CCDT (Client Channel Definition Table), DNS (Domain Name settings), směrování v síti nebo ekvivalentní informace o připojení.

m) Proveďte spravované překonání selhání správce front pro každý uzel RDQM, abyste se ujistili, že požadovaná konfigurace byla úspěšně vytvořena, viz “Nastavení upřednostňované lokality pro RDQM” na stránce 566.

Změna velikosti systému souborů pro správce front HA RDQM
Chcete-li změnit velikost systému souborů pro existujícího správce front replikovaných dat vysoké dostupnosti (RDQM), který zálohujete jeho trvalá data, obnovte data do nově vytvořeného správce front RDQM, který má stejný název, ale jinou velikost systému souborů.

Informace o této úloze

Správci front replikovaných dat HA vyžadují vyhrazený logický svazek (systém souborů) a konfiguraci replikace disku a řízení HA. Tyto komponenty jsou konfigurovány pouze při vytvoření nového správce front. Po vytvoření systému souborů nelze změnit jeho velikost, protože musí mít na každém uzlu stejnou velikost. Chcete-li změnit velikost systému souborů pro existujícího správce front replikovaných dat (RDQM), můžete zálohovat jeho trvalá data a poté obnovit data do nově vytvořeného správce front RDQM, který má stejný název, ale jiný systém souborů jiné velikosti. Tento postup zachovává konfiguraci, stav a trvalé zprávy správce front v době vytvoření zálohy.

Postup

1. Zazálohujte existujícího správce front RDQM na primárním uzlu RDQM:

a) Určete primární uzel RDQM pro správce front. Informace o tom, jak určit primární uzel, viz rdqmstatus (zobrazení stavu RDQM) .

b) Pokud je v primárním uzlu RDQM spuštěn správce front RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .

c) Určete umístění datového adresáře správce front zobrazením konfiguračního souboru IBM MQ `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`viz “IBM MQ konfigurační soubor mqs.ini” na stránce 85.

Vyhledejte sekci `QueueManager` pro správce front v souboru. Datový adresář správce front je hodnota klíče s názvem `DataPath`. Další informace o sekci `QueueManager` viz “QueueManager sekce souboru mqs.ini” na stránce 95.

d) Vytvořte zálohu datového adresáře správce front. V systému Linuxto můžete provést pomocí příkazu **tar** . Chcete-li například zálohovat datový adresář pro správce front, můžete použít následující příkaz. Povšimněte si posledního parametru příkazu, který je jedním znakem tečky (.):

```
tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
```

e) Určete umístění adresáře protokolu správce front zobrazením IBM MQ konfiguračního souboru správce front `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front, qm.ini” na stránce 97.

Adresář protokolu správce front je definován jako hodnota klíče `LogPath` v sekci Protokol. Informace o sekci viz “Sekce protokolu souboru qm.ini” na stránce 130.

f) Vytvořte zálohu adresáře protokolu správce front. V systému Linuxto můžete provést pomocí příkazu **tar** . Chcete-li například zálohovat adresář protokolu pro správce front, můžete použít následující příkaz. Povšimněte si posledního parametru příkazu, který je jedním znakem tečky (.):

```
tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
```

g) Odstraňte existujícího správce front RDQM.

2. Obnovte správce front s požadovaným systémem souborů:

a) Vytvořte nového správce front RDQM se stejným názvem jako zálohovaný správce front. Ujistěte se, že systém souborů přidělený pro správce front RDQM produktem **crtmqm** má požadovanou velikost a že je dostatečně velký na to, aby obsahoval data, primární protokoly a sekundární protokoly pro existujícího správce front, plus další prostor pro budoucí rozšíření. Informace o vytvoření správce front RDQM viz “Vytvoření HA RDQM” na stránce 558.

b) Určete primární uzel RDQM pro správce front. Informace o tom, jak určit primární uzel, viz rdqmstatus (zobrazení stavu RDQM).

c) Pokud je v primárním uzlu RDQM spuštěn správce front RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .

d) V primárním uzlu RDQM určete nové umístění adresářů dat a protokolů pro správce front RDQM (použijte metody popsané v krocích 1c a 1e).

e) V primárním uzlu RDQM odstraňte obsah dat a adresářů protokolu správce front RDQM, nikoli však samotné adresáře.

f) V primárním uzlu RDQM obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a zajistěte zachování vlastnictví souboru a oprávnění. Pokud byla záloha vytvořena pomocí příkladu příkazu **tar** v kroku 1d , může uživatel root k její obnově použít následující příkaz:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

g) V primárním uzlu RDQM obnovte zálohu adresáře protokolu správce front do prázdného adresáře protokolu pro nového správce front RDQM a zajistěte zachování vlastnictví souborů a oprávnění. Pokud byla záloha vytvořena pomocí příkladu příkazu **tar** v kroku 1f , může uživatel root k její obnově použít následující příkaz:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

h) V primárním uzlu RDQM upravte obnovený konfigurační soubor správce front `qm.ini`v datovém adresáři pro nového správce front RDQM. Aktualizujte hodnotu klíče `LogPath` v sekci `Log` tak, aby uváděla adresář protokolu pro nového správce front RDQM, kterého jste určili v kroku 2d. Přezkoumejte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Můžete například potřebovat aktualizovat následující cesty:

- Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
- Cesta pro uživatelské procedury, které jsou vyžadovány správcem front.
- Cesta k souborům načtení přepínače, pokud je správcem front koordinátor transakcí XA.

i) Ověřte, že je správce front zobrazen příkazem **dspmq** a jeho stav je ohlášen jako ukončený. Následující příklad ukazuje ukázkový výstup pro správce front RDQM HA:

```
$ dspmq -o status -o ha
QMNAME(QM1) STATUS(Ended normally) HA(Replicated)
```

j) Pomocí příkazu **rdqmstatus** ověřte, zda byla obnovená data správce front replikována do sekundárních uzlů RDQM, a zobrazte tak stav správce front. Stav HA by měl být nahlášen jako `Normal` na každém uzlu. Následující příklad ukazuje ukázkový výstup pro správce front RDQM HA:

```
$ rdqmstatus -m QM1
Node: mqhavm10-adm
Queue manager status:         Ended normally
Queue manager file system:    50MB used, 0.2GB
allocated [42%]
HA role:                      Primary
HA status:                    Normal
HA control:                   Disabled
HA current location:          This node
HA preferred location:        This node
HA floating IP interface:     None
HA floating IP address:       None
Node:                         mqhavm11-adm
HA status:                    Normal
Node:                         mqhavm12-adm
HA status:                    Normal
```

k) Spusťte správce front v primárním uzlu RDQM.

l) Proveďte spravované překonání selhání správce front pro každý uzel RDQM, abyste se ujistili, že požadovaná konfigurace byla úspěšně vytvořena, viz “Nastavení upřednostňované lokality pro RDQM” na stránce 566.

Ukládání stavu trvalé aplikace
Můžete uložit informace o trvalém stavu týkající se aplikací spolu s dalšími daty správce front.

Každý správce front IBM MQ má vyhrazený systém souborů pro svůj trvalý stav, který zahrnuje jak data fronty, tak protokol zotavení. V konfiguraci RDQM je systém souborů zálohován logickým svazkem, který je replikován mezi systémy Linux (uzly). Systém souborů obsahuje adresář `userdata` , který můžete použít k uložení informací o trvalém stavu pro vaše aplikace. Takže když se správce front replikovaných dat přesune ke spuštění v jiném uzlu v konfiguraci RDQM, máte k dispozici kontext aplikace i kontext správce front. Viz Obsah adresáře v systémech Unix a Linux Systems.

Pokud se rozhodnete uložit stav aplikace do adresáře `userdata` , musíte si uvědomit, že data zapsaná do tohoto umístění mohou spotřebovat dostupné místo na disku přidělené správci front. Je třeba zajistit, aby byl pro správce front k dispozici dostatek místa na disku pro zápis dat fronty, protokolů a dalších informací o trvalém stavu.

Adresář `userdata` má vlastnictví uživatele mqm a skupiny a je čitelný, takže k němu mohou uživatelé přistupovat, aniž by museli být ve skupině administrátorů IBM MQ (tj. mqm). Nemůžete upravit oprávnění adresáře `userdata` , ale můžete v něm vytvořit obsah s libovolným vlastnictvím a oprávněními, která požadujete.

Během překonání selhání správce front RDQM je správce front ukončen a jeho systém souborů je odpojen od aktuálního uzlu RDQM. Systém souborů je poté připojen a správce front je restartován

v jiném uzlu v konfiguraci RDQM. Systém souborů nelze odpojit, pokud má proces otevřený popisovač pro jeden ze svých souborů. Chcete-li zajistit dokončení překonání selhání správce front, v případě, že systém souborů správce front nelze odpojit, budou procesům s otevřenou manipulací se odešle signál SIGTERM následovaný signálem SIGKILL, nejsou-li otevřené manipulátory uvolněny. Vaše aplikace musí být navrženy tak, aby správně reagovaly na SIGTERM. Jsou-li aplikace nebo procesy konfigurovány jako služba správce front, mohou být během spravovaného překonání selhání ukončeny během ukončování činnosti správce front před odpojením systému souborů. Pokud aplikace nebo proces není konfigurován jako služba správce front nebo dojde k nespravovanému překonání selhání, například ke ztrátě kvora, pak je pravděpodobné, že budou odeslány signály pro uvolnění systému souborů.

Linux *Nastavení upřednostňované lokality pro RDQM*

Upřednostňované umístění pro správce front replikovaných dat (RDQM) identifikuje uzel, kde by měl být spuštěn RDQM, je-li tento uzel k dispozici.

Informace o této úloze

Upřednostňované umístění je název uzlu, na kterém by měl modul Pacemaker spustit správce front, když je skupina HA v normálním stavu (všechny uzly a připojení jsou k dispozici). Upřednostňované umístění je při vytvoření správce front inicializováno na název primárního uzlu. Můžete spustit příkazy pro nastavení upřednostňovaného umístění na libovolném ze tří uzlů. Musíte být uživatel, který patří do skupin `mqm` i `haclient` .

Procedura

- Chcete-li přiřadit lokální nebo určený uzel jako upřednostňované umístění pro uvedeného správce front, zadejte následující příkaz:

  ```
  rdqmadm -p -m qmname [ -n nodename[,nodename  ]
  ```

  kde *qmname* je název RDQM, pro který zadáváte upřednostňované umístění, a *nodename* je volitelně název upřednostňovaného uzlu.

  Pokud se skupina HA nachází v normálním stavu a upřednostňované umístění není aktuálním primárním uzlem, správce front se zastaví a restartuje v novém upřednostňovaném umístění. Můžete zadat seznam dvou názvů uzlů oddělených čárkami, chcete-li přiřadit druhou předvolbu upřednostňovaného umístění.
- Chcete-li vymazat upřednostňované umístění, aby se správce front při obnově automaticky nevracel do uzlu, zadejte následující příkaz:

  ```
  rdqmadm -p -m qmname -d
  ```

Související odkazy

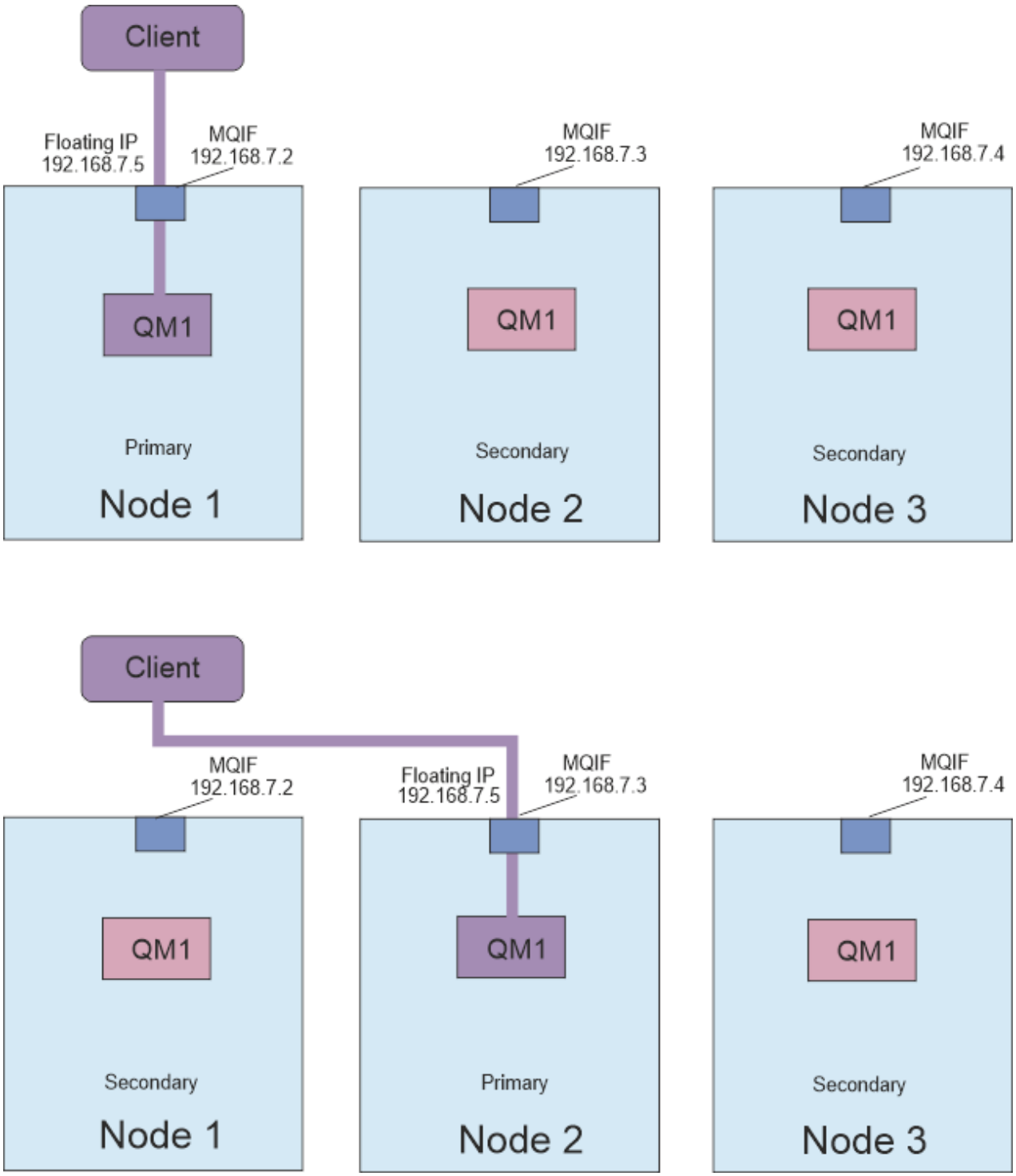
rdqmadm (spravovat klastr správce front replikovaných dat)

Linux *Vytvoření a odstranění plovoucí adresy IP*

Plovoucí adresa IP umožňuje klientovi používat stejnou adresu IP pro správce front replikovaných dat (RDQM) bez ohledu na to, na kterém uzlu ve skupině HA je spuštěn. (Použití plovoucí adresy IP je volitelné.)

Informace o této úloze

Plovoucí adresu IP můžete vytvořit nebo odstranit pomocí příkazu **rdqmint** . Plovoucí adresa se váže na pojmenované fyzické rozhraní na primárním uzlu pro RDQM. Pokud dojde k selhání RDQM a jiný uzel se stane primárním uzlem, plovoucí adresa IP je svázána s rozhraním se stejným názvem na novém primárním uzlu. Fyzická rozhraní na třech uzlech musí patřit do stejné podsítě jako plovoucí adresa IP. Následující diagram ilustruje použití plovoucí adresy IP.



Obrázek 80. Plovoucí adresa IP

Chcete-li spustit příkaz **rdqmint** , musíte být uživatelem ve skupinách `mqm` i `haclient` . Můžete vytvořit nebo odstranit plovoucí adresu IP na primárním uzlu pro RDQM nebo na jednom ze sekundárních uzlů.

Poznámka: Nemůžete použít stejnou plovoucí adresu IP pro více RDQM, plovoucí adresa IP pro každý RDQM musí být jedinečná.

Procedura

- Chcete-li vytvořit plovoucí adresu IP pro RDQM, zadejte následující příkaz:

```
rdqmint -m qmname -a  -f ipv4address -l interfacename
```

kde:

QMNAME
Název RDQM, pro který vytváříte plovoucí adresu IP.

ipv4address
Plovoucí adresa IP ve formátu ipv4 .

Plovoucí adresa IP musí být platnou adresou IPv4 , která již není definována na žádném uzlu HA, a musí patřit do stejné podsítě jako statické adresy IP definované pro lokální rozhraní.

interfaceName
Název fyzického rozhraní na primárním uzlu, se kterým se má vytvořit vazba.

Příklad:

```
rdqmint -m QM1 -a -f 192.168.7.5 -l MQIF
```

- Chcete-li odstranit existující plovoucí adresu IP, zadejte následující příkaz:

```
rdqmint -m qmname -d
```

Související odkazy
rdqmint (přidat nebo odstranit plovoucí adresu IP pro RDQM)

Linux *Spuštění, zastavení a zobrazení stavu HA RDQM*

Varianty standardních řídicích příkazů IBM MQ se používají ke spuštění, zastavení a zobrazení aktuálního stavu správce front replikovaných dat (RDQM).

Informace o této úloze

Musíte spustit příkazy, které spustí, zastaví a zobrazí aktuální stav správce front replikovaných dat (RDQM) jako uživatel, který patří do skupin `mqm` i `haclient` .

Musíte spustit příkazy pro spuštění a zastavení správce front v primárním uzlu pro tohoto správce front.

Procedura

- Chcete-li spustit RDQM, zadejte na primárním uzlu RDQM následující příkaz:

```
strmqm qmname
```

kde *qmname* je název RDQM, který chcete spustit.

Je spuštěn RDQM a Pacemaker spustí správu RDQM. Chcete-li zadat další volby `strmqm` , musíte zadat volbu `-ns` spolu s volbou `strmqm` .

- Chcete-li zastavit RDQM, zadejte na primárním uzlu RDQM následující příkaz:

```
endmqm qmname
```

kde *qmname* je název RDQM, který chcete zastavit.

Modul Pacemaker ukončí správu RDQM a poté je RDQM ukončen. Všechny ostatní parametry **endmqm** lze použít při zastavování RDQM.

- Chcete-li zobrazit stav RDQM, zadejte následující příkaz:

```
dspmq
```

Výstupní informace o stavu závisí na tom, zda jste spustili příkaz na primárním nebo sekundárním uzlu RDQM. Pokud se spustí na primárním uzlu, zobrazí se jedna z běžných stavových zpráv vrácených

produktem **dspmq** . Spustíte-li příkaz na sekundárním uzlu, zobrazí se stav `running elsewhere` . Pokud je například produkt **dspmq** spuštěn na uzlu RDQM7, mohou být vráceny následující informace:

```
QMNAME(RDQM8)                             STATUS(Running elsewhere)
QMNAME(RDQM9)                             STATUS(Running elsewhere)
QMNAME(RDQM7)                             STATUS(Running)
```

Není-li primární uzel k dispozici nebo je-li **dspmq** spuštěn uživatelem, který není `root` , nebo členem skupiny `haclient` , je nahlášen stav `Unavailable` . Příklad:

```
QMNAME(RDQM8)               STATUS(Unavailable)
QMNAME(RDQM9)               STATUS(Unavailable)
QMNAME(RDQM7)               STATUS(Unavailable)
```

Zadáním příkazu **dspmq -o ha** (nebo **dspmq -o HA**) můžete zobrazit seznam správců front známých uzlu, a zda se jedná o RDQMs, či nikoli, například:

```
dspmq -o ha

QMNAME(RDQM8)                                         HA(Replicated)
QMNAME(RDQM9)                                         HA(Replicated)
QMNAME(RDQM7)                                         HA(Replicated)
QMNAME(QM7)                                           HA()
```

Související odkazy

dspmq (zobrazení správců front)

endmqm (koncový správce front)

strmqm (spustit správce front)

V 9.3.0 *Nezdařené akce prostředků*

Akce nezdařených prostředků se vyskytnou, když komponenta Pacemaker konfigurace vysoké dostupnosti RDQM zjistí nějaký problém s prostředkem na jednom z uzlů ve skupině HA.

Řešení RDQM HA používá Pacemaker pro monitorování a správu prostředků (viz “Vysoká dostupnost RDQM” na stránce 549). Pokud modul Pacemaker zjistí chybu při provádění operace na prostředku v uzlu, zaznamená tyto informace pomocí akce nezdařeného prostředku. Některé nezdařené akce prostředku brání spuštění prostředku a musí být vymazány, aby mohl modul Pacemaker prostředek restartovat.

Pomocí příkazu **rdqmstatus -m** můžete zjistit, zda existují nějaké nezdařené akce prostředků, které zastavují spuštění správce front na jednom nebo více uzlech.

Poté můžete pomocí příkazu **rdqmstatus -m** *qmname* **-a** zobrazit podrobnosti o akcích nezdařených prostředků, které jsou přidruženy ke správci front. Postupujte podle této akce pomocí příkazu **rdqmclean** , abyste vymazali tyto nezdařené akce prostředků, a tak uvolněte všechny omezené prostředky. (Musíte také provést akci, abyste vyřešili problémy, které způsobily akci nezdařeného prostředku.)

Následující prostředky jsou řízeny produktem Pacemaker v konfiguraci RDQM HA a mohou být předmětem nezdařených akcí prostředků:

- Správce front
- Plovoucí adresa IP
- Řízení RDQM
- Systém souborů
- Replikace DR (DRBD)
- Replikace HA (DRBD)

Každý typ prostředku může být předmětem následujících typů selhání:

Měkký
Měkká selhání jsou dočasná a modul Pacemaker se nadále pokouší obnovit prostředek, dokud nevypne časový limit nebo dokud není jinak zastaven.

Obtížný
Tvrdá chyba vyžaduje administrativní zásah. Pevné chyby blokují spuštění prostředku na konkrétním uzlu.

Kritická
Závažná chyba vyžaduje administrativní zásah. Závažné chyby blokují spuštění prostředku na libovolném uzlu.

Příklady stavu včetně nezdařených akcí ve frontě prostředků viz “Zobrazení stavu skupiny RDQM a HA” na stránce 570 .

Pomocí příkazu **rdqmclean** můžete vymazat všechny nezdařené akce prostředků přidružené k určenému správci front nebo všechny nezdařené akce prostředků v konfiguraci RDQM HA.

Poznámka: Některé nezdařené akce prostředků nevedou k zablokování správce front v uzlu. Například po neočekávaném ukončení správce front se modul Pacemaker pokusí restartovat správce front v uzlu, v němž bylo zjištěno, že není spuštěn. Pokud je spuštění úspěšné, není spuštění správce front v uzlu blokováno. Jediný způsob, jak byste se v tomto případě dozvěděli o akci nezdařeného prostředku, je spuštění příkazu **rdqmstatus -m** *qmname* **-a**.

Související úlohy
“Zobrazení stavu skupiny RDQM a HA” na stránce 570
Můžete zobrazit stav skupiny HA a jednotlivých správců front replikovaných dat (RDQM).

Související odkazy
rdqmclean
rdqmstatus

Linux *Zobrazení stavu skupiny RDQM a HA*

Můžete zobrazit stav skupiny HA a jednotlivých správců front replikovaných dat (RDQM).

Informace o této úloze

Příkaz **rdqmstatus** použijete k zobrazení stavu jednotlivých RDQM a skupiny HA jako celku.

V 9.3.0 Souhrnný stav uzlu také zobrazuje informace o modulu jádra DRBD, na kterém RDQM spoléhá. Při upgradu RDQM je důležité zajistit, aby byla pro verzi jádra RHEL spuštěného v systému nainstalována správná verze modulu jádra DRBD. Stav zobrazuje verzi jádra operačního systému, verzi jádra, pro kterou byl modul DRBD sestaven, verzi DRBD a stav načtení modulu jádra DRBD.

Chcete-li spustit příkaz **rdqmstatus** , musíte být uživatelem ve skupinách `mqm` a `haclient` . Příkaz můžete spustit na libovolném ze tří uzlů.

Procedura

- Chcete-li zobrazit souhrnný stav uzlu a RDQM, které jsou součástí konfigurace vysoké dostupnosti, postupujte takto:

  ```
  rdqmstatus
  ```

  Zobrazí se identita uzlu, který jste spustili v systému, podrobnosti jádra a DRBD pro daný uzel a stav RDQMs v konfiguraci vysoké dostupnosti, například:

  ```
  Node:                                mqhavm07.exampleco.com
  OS kernel version:                   3.10.0-1160.15.2
  DRBD OS kernel version:              3.10.0-1160
  DRBD version:                        9.1.1
  DRBD kernel module status:           Loaded

  Queue manager name:                  RDQM8
  Queue manager status:                Running elsewhere
  HA current location:                 mqhavm08.exampleco.com
  HA preferred location:               mqhavm08.exampleco.com
  HA blocked location:                 None
  ```

```
Queue manager name:                     RDQM9
Queue manager status:                   Running elsewhere
HA current location:                    mqhavm09.exampleco.com
HA preferred location:                  mqhavm09.exampleco.com
HA blocked location:                    None

Queue manager name:                     RDQM7
Queue manager status:                   Running
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
```

V 9.3.0 Stav modulu jádra DRBD je jedna z následujících hodnot:

Načteno
Označuje, že byl načten modul DRBD.

Částečně načteno
Může se vyskytnout, když byl modul DRBD načten, ale nefunguje správně kvůli neshodě.

Nenačteno
Modul DRBD není načten. Tuto možnost lze zobrazit v nově nainstalované konfiguraci v případě, že dosud nebyli vytvořeni žádní správci front RDQM.

Neinstalováno
Označuje, že buď modul DRBD není nainstalován. nebo že produkt IBM MQ nemohl určit verzi jádra operačního systému modulu DRBD.

Dříve nainstalovaná verze je stále načtena
Tento stav může nastat, pokud je nainstalován nový modul DRBD, zatímco je spuštěn existující modul DRBD (tj. je spuštěn správce front RDQM). Nově nainstalovaný modul je ohlášen ve stavu, ale nejedná se o modul, který je ve skutečnosti spuštěn.

- Chcete-li zobrazit stav tří uzlů ve skupině HA, zadejte následující příkaz:

```
rdqmstatus -n
```

Je ohlášen stav online nebo offline každého uzlu. Příklad:

```
Node mqha04(mqhavm04.example.com) is online
Node mqha05(mqhavm05.example.com) is offline
Node mqha06(mqhavm06.example.com) is online
```

- Chcete-li zobrazit stav konkrétního správce front na všech uzlech ve skupině s vysokou dostupností, zadejte následující příkaz:

```
rdqmstatus -m qmname
```

kde *qmname* je název RDQM, pro který chcete zobrazit stav. Zobrazí se stav RDQM na aktuálním uzlu následovaný souhrnem stavu ostatních dvou uzlů z perspektivy aktuálního uzlu.

- V 9.3.0
Chcete-li zobrazit stav konkrétního správce front na všech uzlech ve skupině s vysokou dostupností, včetně podrobností o všech nezdařených akcích prostředků, zadejte následující příkaz:

```
rdqmstatus -m qmname -a
```

kde *qmname* je název RDQM, pro který chcete zobrazit stav. Zobrazí se stav RDQM na aktuálním uzlu následovaný souhrnem stavu ostatních dvou uzlů z perspektivy aktuálního uzlu. Za tím následují podrobnosti o všech nezdařených akcích prostředků přidružených k RDQM.

- Následující tabulka shrnuje informace o aktuálním uzlu, které mohou být vráceny příkazem `rdqmstatus -m qmname` pro RDQM.

Tabulka 32. Aktuální stav uzlu		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Název uzlu	*NodeName*	Vždy zobrazeno
Stav správce front	Spuštěno Spuštěno jinde Ukončeno Není k dispozici	Vždy zobrazeno
CPU	*n.nn*%	Zobrazí se pouze, když má aktuální uzel primární roli (to znamená, že RDQM je spuštěn na tomto uzlu)
Paměť	*nnn*využitých MB, *y.y*přidělených GB	Zobrazí se pouze, když má aktuální uzel primární roli (to znamená, že RDQM je spuštěn na tomto uzlu)
Systém souborů správce front	*nnn*použitých MB, *y.y*přidělených GB [*z*%]	Zobrazí se pouze, když má aktuální uzel primární roli (to znamená, že RDQM je spuštěn na tomto uzlu)
Role HA	Primární sekundární neznámý	Vždy zobrazeno
Stav HA	Všechny uzly jsou v pohotovostním režimu Tento uzel je v pohotovostním režimu Vzdálené uzly v pohotovostním režimu Smíšená *stav vzdálených uzlů*	Všechny uzly jsou v pohotovostním režimu Aktuální uzel v pohotovostním režimu Oba vzdálené uzly v pohotovostním režimu Jiný stav pro každý vzdálený uzel (individuální stav viz další tabulka) Stejný stav pro oba vzdálené uzly (viz další tabulka pro všechny hodnoty)
Řízení HA	Povoleno Zakázáno Neznámý	Vždy zobrazeno. Zobrazuje, zda je RDQM pod ovládacím prvkem Pacemaker
Upřednostňované umístění HA	Není Tento uzel Neznámý *NodeName*	Vždy zobrazeno

Tabulka 32. Aktuální stav uzlu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
V 9.3.0 V 9.3.0 Blokované umístění vysoké dostupnosti	Žádný-Správce front není blokován ke spuštění v žádném uzlu Tento uzel-správci front je zablokováno spuštění v aktuálním uzlu kvůli jedné nebo více nezdařeným akcím prostředků *nodename* -Správce front je blokován před spuštěním na *nodename* kvůli jedné nebo více nezdařeným akcím prostředků. *nodename1*, *nodename2* -Správce front je blokován před spuštěním v systému *nodename1* a *nodename2* kvůli jedné nebo více nezdařeným akcím prostředku. Všechny uzly-správci front je zablokováno spuštění ve všech uzlech kvůli jedné nebo více nezdařeným akcím prostředků.	Vždy zobrazeno
Plovoucí rozhraní IP HA	*název_rozhraní*	Vždy zobrazeno
Plovoucí adresa IP HA	*IPV4_address*	Vždy zobrazeno

Následující tabulka shrnuje informace, které jsou vráceny příkazem `rdqmstatus -m` *qmname* pro ostatní uzly ve skupině HA.

Tabulka 33. Stav jiného uzlu		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Název uzlu	*nodename*	Vždy zobrazeno
Stav HA	Normální Probíhá synchronizace Vzdáleně nedostupné Nekonzistentní Pozastaveno Vzdálený uzel je v pohotovostním režimu Neznámý	Uzly jsou navzájem synchronizovány Synchronizace se vzdáleným uzlem Nelze komunikovat se vzdáleným uzlem Nesynchronizováno se vzdáleným uzlem a nesynchronizováno Replikace pozastavena Vzdálený uzel je v pohotovostním režimu
Probíhá synchronizace HA	*n.n*%	Zobrazí se, když probíhá synchronizace, a příkaz se spustí jako `root`
Odhadovaný čas synchronizace HA	*rrrr-mm-dd hh:mm:ss.nnn*	Zobrazeno při probíhající synchronizaci
Nesynchronizovaná data HA	*n*KB	Zobrazí se, když je vzdálený uzel nedostupný nebo nekonzistentní

Tabulka 33. Stav jiného uzlu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
V 9.3.0 V 9.3.0 Poslední synchronizace HA	*rrrr-mm-dd hh:mm:ss.nnn*	Zobrazí se, když jsou data HA nesynchronizovaná (po počáteční synchronizaci). Udává čas a datum, kdy byla data naposledy synchronizována.

Příklad

Příklad normálního stavu na primárním uzlu:

```
Node:                                  mqhavm07.exampleco.com
Queue manager status:                   Running
CPU:                                    0.00
Memory:                                 123MB
Queue manager file system:              606MB used, 1.0GB allocated [60%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               eth4
HA floating IP address:                 192.0.2.4


Node:                                   mqhavm08.exampleco.com
HA status:                              Normal


Node:                                   mqhavm09.exampleco.com
HA status:                              Normal
```

Příklad normálního stavu na sekundárním uzlu:

```
Node:                                   mqhavm08.exampleco.com
Queue manager status:                   Running elsewhere
HA role:                                Secondary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    mqhavm07.exampleco.com
HA preferred location:                  mqhavm07.exampleco.com
HA blocked location:                    None
HA floating IP interface:               eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm07.exampleco.com
HA status:                              Normal

Node:                                   mqhavm09.exampleco.com
HA status:                              Normal
```

Příklad stavu na primárním uzlu při probíhající synchronizaci:

```
Node:                                   mqhavm07.exampleco.com
Queue manager status:                   Running
CPU:                                    0.53
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Synchronization in progress
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm08.exampleco.com
HA status:                              Synchronization in progress
```

```
HA synchronization progress:            11.0%
HA estimated time to completion:        2017-09-06 14:55:05

Node:                                   mqhavm09.exampleco.com
HA status:                              Synchronization in progress
HA synchronization progress:            11.0%
HA estimated time to completion:        2017-09-06 14:55:06
```

V 9.3.0 Příklad stavu na primárním uzlu při ztrátě synchronizace:

```
Node:                                   mqhavm07.exampleco.com
Queue manager status:                   Running
CPU:                                    0.53
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Mixed
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm08.exampleco.com
HA status:                              Normal

Node:                                   mqhavm09.exampleco.com
HA status:                              Inconsistent
HA out of sync data:                    15932KB
HA last in sync:                        2017-09-06 14:55:06
```

Příklad primárního uzlu s více stavy:

```
Node:                                   mqhavm07.exampleco.com
Queue manager status:                   Running
CPU:                                    0.02
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Mixed
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm08.exampleco.com
HA status:                              Normal

Node:                                   mqhavm09.exampleco.com
HA status:                              Inconsistent
```

V 9.3.0 Příklad primárního uzlu, který zobrazuje nezdařené akce prostředků:

```
Node:                                   mqhavm07.exampleco.com
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              606MB used, 1.0GB allocated [60%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  mqhavm08.exampleco.com
HA blocked location:                    mqhavm08.exampleco.com
HA floating IP interface:               eth4
HA floating IP address:                 192.0.2.4

Node:                                   mqhavm08.exampleco.com
HA status:                              Normal

Node:                                   mqhavm09.exampleco.com
HA status:                              Normal

Failed resource action:                 Start
```

```
Resource type:                          Filesystem
Failure node:                           mqhavm08.exampleco.com
Failure time:                           2017-09-06 12:00:00
Failure reason:                         Couldn't find directory  [/var/mqm/vols/qmname] to use
as a mount point
Blocked location:                       mqhavm08.exampleco.com
```

Tento stav ukazuje, že modul Pacemaker nebyl schopen spustit systém souborů na uzlu mqhavm08.exampleco.com ve 12:00:00. Tato akce nezdařených prostředků znamená, že spuštění správce front v systému mqhavm08.exampleco.comje blokováno. Po vyřešení základního problému, který způsobil selhání akce prostředku, spusťte příkaz **rdqmclean** a vymažte akci, která se nezdařila, aby mohl modul Pacemaker zopakovat akci (je-li to nutné).

V 9.3.0 Příklad souhrnného stavu, který ukazuje neshodu mezi verzí jádra operačního systému (RHEL 7.9) a modulem jádra DRBD (zaměřeno na RHEL 7.8). I když zpráva o stavu hlásí, že je načten modul jádra DRBD a je spuštěn správce front, měli byste aktualizovat modul jádra DRBD o verzi, která je v této situaci určena pro spuštěné jádro operačního systému.

```
Node:                                   mqhavm07.exampleco.com
OS kernel version:                      3.10.0-1160.15.2
DRBD OS kernel version:                 3.10.0-1127
DRBD version:                           9.1.1
DRBD kernel module status:              Loaded

Queue manager name:                     RDQM7
Queue manager status:                   Running
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
```

V 9.3.0 Příklad souhrnného stavu ukazujícího neshodu mezi verzí jádra operačního systému (RHEL 7.9) a modulem jádra DRBD (zaměřeným na RHEL 7.6). V tomto příkladu je neshoda verzí závažnější a modul jádra DRBD se nepodařilo úspěšně načíst. V důsledku toho se správci front nedaří spustit v upřednostňovaném uzlu a ve stavu vysoké dostupnosti v produktu Unknown. Chcete-li toto selhání vyřešit, musí být modul jádra DRBD aktualizován s cílem verze pro spuštěné jádro operačního systému.

```
Node:                                   mqhavm57.exampleco.com
OS kernel version:                      3.10.0-1160.15.2
DRBD OS kernel version:                 3.10.0-957
DRBD version:                           9.1.2+ptf.3
DRBD kernel module status:              Partially loaded

Queue manager name:                     QM2
Queue manager status:                   Running elsewhere
HA status:                              Unknown
HA current location:                    mqhavm58.exampleco.com
HA preferred location:                  This node
HA blocked location:                    All nodes
```

Související odkazy

Linux rdqmstatus

Změna adres IP v konfiguracích vysoké dostupnosti

Změníte-li adresy IP některého z rozhraní v konfiguraci vysoké dostupnosti, operace vysoké dostupnosti již nebude k dispozici a správce front nebude spuštěn v uzlu, v němž byly adresy změněny.

Pro operaci vysoké dostupnosti v souboru `rdqm.ini` uvedete až tři adresy IP. Pokud jste již změnili adresy monitoru Pacemaker , musíte je před provedením postupu dočasně obnovit na původní hodnoty. Jinak není možné odstranit správce front HA RDQM.

1. Odeberte konfiguraci vysoké dostupnosti na každém uzlu. Vysokou dostupnost odeberete zálohováním správců front a jejich odstraněním, viz “Zálohování a obnova dat správce front IBM MQ” na stránce 650 a “Odstranění RDQM s vysokou dostupností” na stránce 560a následným odebráním samotné skupiny vysoké dostupnosti, viz “Odstranění klastru Pacemaker (skupina HA)” na stránce 558.

2. Znovu vytvořte konfiguraci vysoké dostupnosti s novými adresami IP, viz “Definování klastru Pacemaker (skupina HA)” na stránce 554.
3. Znovu vytvořte správce front HA a obnovte zálohu, viz “Vytvoření HA RDQM” na stránce 558 a “Zálohování a obnova dat správce front IBM MQ” na stránce 650.

Linux *Nahrazení uzlu, u kterého došlo k selhání, v konfiguraci vysoké dostupnosti*

Pokud jeden z uzlů ve vaší skupině HA selže, můžete jej nahradit.

Informace o této úloze

Postup při nahrazení uzlu závisí na scénáři:

- Pokud nahrazujete uzel, u kterého došlo k selhání, uzlem s identickou konfigurací, můžete uzel nahradit bez narušení skupiny HA.
- Pokud má nový uzel jinou konfiguraci, musíte odstranit a znovu sestavit skupinu HA. Nejprve můžete zálohovat správce front z uzlu, na kterém jsou spuštěni, a poté je obnovit po opětovném sestavení skupiny HA.

Procedura

- Je-li náhradní uzel nakonfigurován tak, aby vypadal jako uzel, který selhal (stejný název hostitele, stejné adresy IP atd.), postupujte na novém uzlu takto:
  a) Vytvořte soubor `rdqm.ini` , který odpovídá souborům na ostatních uzlech, a pak spusťte příkaz `rdqmadm -c` (viz “Definování klastru Pacemaker (skupina HA)” na stránce 554).
  b) Spusťte příkaz `crtmqm -sxs` *`qmanager`* a znovu vytvořte jednotlivé správce front replikovaných dat (viz “Vytvoření HA RDQM” na stránce 558).
- Pokud má náhradní uzel jinou konfiguraci než uzel, který selhal:
  a) V případě potřeby zazálohujte správce front (viz “Zálohování a obnova dat správce front IBM MQ” na stránce 650).
  b) Odstraňte správce front replikovaných dat z ostatních uzlů ve skupině HA pomocí příkazu **`dltmqm`** (viz “Odstranění RDQM s vysokou dostupností” na stránce 560).
  c) Zrušte konfiguraci klastru Pacemaker pomocí příkazu **`rdqmadm -u`** (viz “Odstranění klastru Pacemaker (skupina HA)” na stránce 558).
  d) Překonfigurujte klastr Pacemaker včetně informací o novém uzlu pomocí příkazu **`rdqmadm -c`** (viz “Definování klastru Pacemaker (skupina HA)” na stránce 554).
  e) V případě potřeby (tj. pokud nemáte přístup SSH k ostatním uzlům) spusťte příkaz `crtmqm -sxs` *`qmanager`* a znovu vytvořte všechny správce front replikovaných dat v ostatních uzlech (viz “Vytvoření HA RDQM” na stránce 558).
  f) Spuštěním příkazu `crtmqm -sx` *`qmanager`*vytvořte správce front v náhradním uzlu.
  g) V případě potřeby obnovte data a konfiguraci pro správce front (viz “Zálohování a obnova dat správce front IBM MQ” na stránce 650).

Linux MQ Adv. Zotavení z havárie RDQM

RDQM (správce front replikovaných dat) je k dispozici na podmnožině platforem Linux a může poskytnout řešení zotavení z havárie.

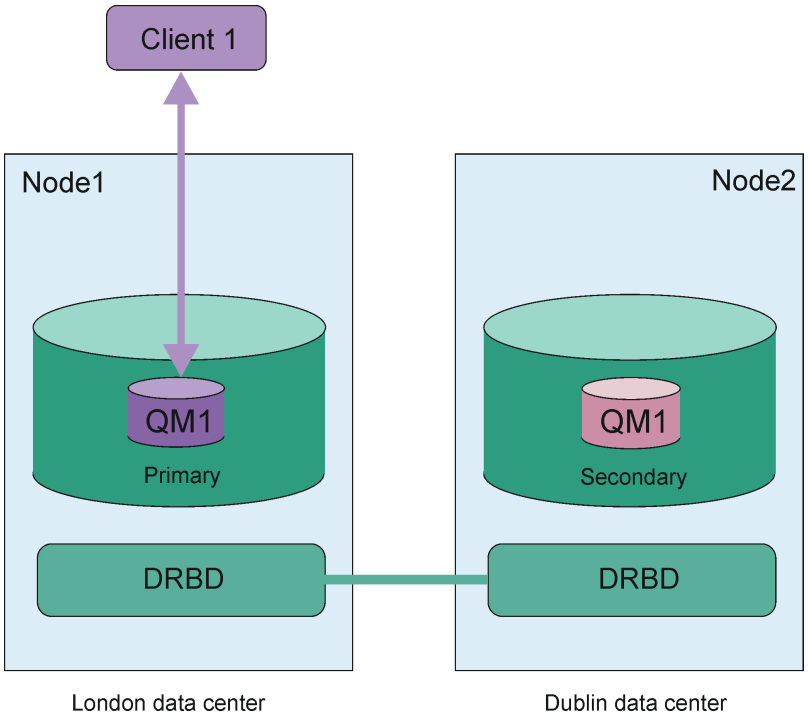
Úplné podrobnosti viz Sestavy kompatibility softwarových produktů .

Můžete vytvořit primární instanci správce front pro zotavení z havárie spuštěného na jednom serveru a sekundární instanci správce front na jiném serveru, který bude fungovat jako uzel zotavení. Data jsou replikována mezi instancemi správce front. Pokud ztratíte primárního správce front, můžete ručně změnit sekundární instanci na primární instanci a spustit správce front a poté obnovit práci ze stejného místa. Správce front nelze spustit, pokud je v sekundární roli. Replikaci dat mezi dvěma uzly zpracovává DRBD.

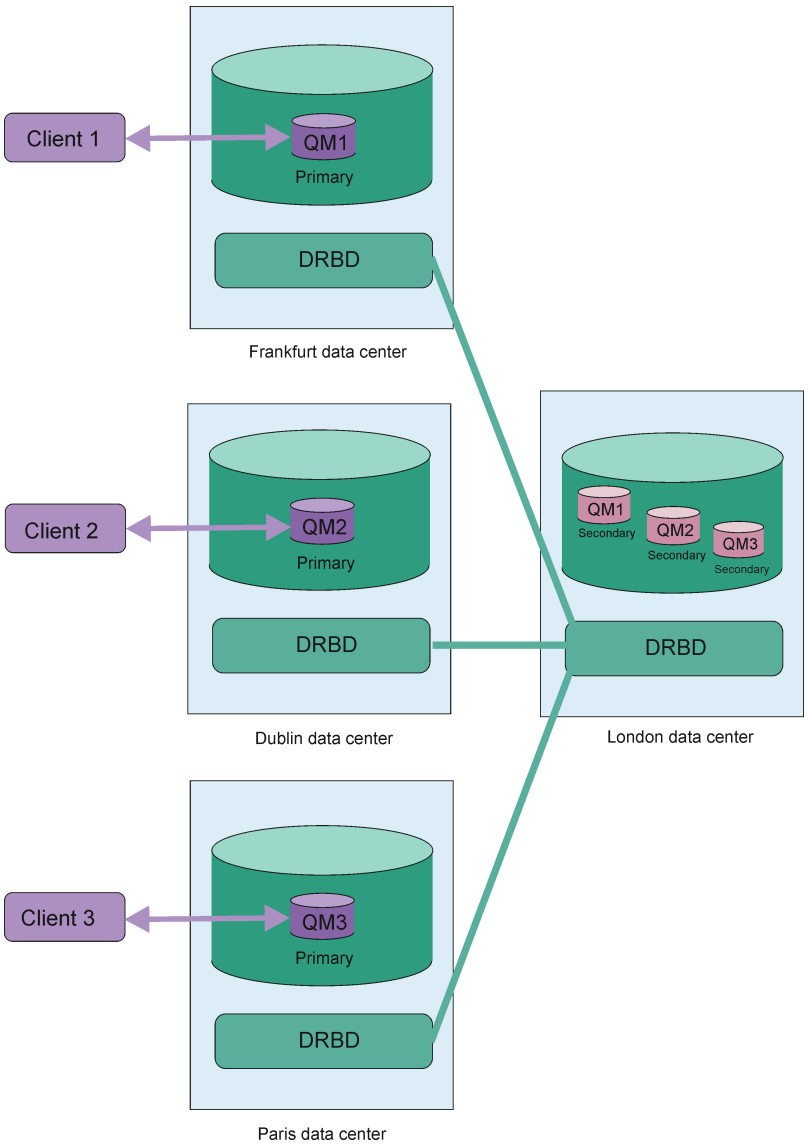
Můžete zvolit mezi synchronní a asynchronní replikací dat mezi primárním a sekundárním správcem front. Vyberete-li asynchronní volbu, operace jako IBM MQ PUT nebo GET se dokončí a vrátí do aplikace před replikací události do sekundárního správce front. Asynchronní replikace znamená, že po situaci zotavení mohou být některá data systému zpráv ztracena. Sekundární správce front však bude v konzistentním stavu a bude schopen okamžitého spuštění, a to i v případě, že je spuštěn v mírně dřívější části proudu zpráv.

Nemůžete přidat zotavení z havárie do existujícího správce front, ačkoli můžete migrovat existujícího správce front, aby se stal správcem front RDQM (viz “Migrace správce front na správce front DR RDQM” na stránce 584).

Můžete mít několik dvojic správců front RDQM spuštěných na řadě různých serverů. Například můžete mít primární správce front pro zotavení z havárie spuštěné na různých uzlech, zatímco všichni jejich sekundární správci front pro zotavení z havárie jsou spuštěni na stejném uzlu. Některé ukázkové konfigurace jsou znázorněny v následujících diagramech.



Obrázek 81. Jedna dvojice RDQM



Obrázek 82. Sekundární správci front ve stejném uzlu

Replikace, synchronizace a snímky

Během připojení dvou uzlů v konfiguraci zotavení z havárie jsou všechny aktualizace trvalých dat pro správce front pro zotavení z havárie přeneseny z primární instance správce front do sekundární instance. Toto je známé jako **replikace**.

Dojde-li ke ztrátě síťového připojení mezi těmito dvěma uzly, budou sledovány změny trvalých dat pro primární instanci správce front. Když je obnoveno síťové připojení, použije se jiný proces k získání sekundární instance tak rychle, jak je to možné. Toto je známé jako **synchronizace**.

Během probíhající synchronizace jsou data na sekundární instanci v nekonzistentním stavu. Je vytvořen **snímek** stavu dat sekundárního správce front. Dojde-li během synchronizace k selhání hlavního uzlu nebo síťového připojení, sekundární instance se vrátí k tomuto snímku a správce front lze spustit. Všechny aktualizace, které se staly od původního selhání sítě, jsou však ztraceny.

Rozdělená data (rozdělený mozek)

Konfigurace RDQM DR vyžadují akci uživatele po ztrátě primární instance správce front pro povýšení a spuštění sekundární instance na uzlu zotavení. Je odpovědností toho, kdo (nebo koho) povyšuje sekundární instanci, aby se ujistil, že je bývalý primární správce front zastaven. Pokud je původní primární

databáze stále spuštěna, může zpracovávat zprávy a při obnovení normální operace mají dvě instance správce front různé pohledy na data. Toto je známé jako rozdělený nebo rozdělený stav mozku.

Zvažte následující situace:

- Uzel, na kterém je spuštěn primární správce front, zcela selhává. Povyšujete sekundární instanci, aby se stala primární; nemůžete provést akci, abyste zastavili původní primární instanci, protože není spuštěna. Když je původní uzel opraven nebo nahrazen, správce front v tomto uzlu se na počátku stane sekundárním a bude synchronizován s primárním správcem front v uzlu zotavení. Role těchto dvou správců front jsou poté obráceny a normální operace se znovu obnoví. Jedinou potenciální ztrátou dat v této situaci jsou jakákoli data, která primární server nedokončil replikaci na sekundární server před selháním uzlu.
- Došlo k selhání sítě, které mělo vliv na propojení replikace mezi uzly, na kterých je spuštěna primární a sekundární instance správce front. V této situaci se musíte ujistit, že jste zastavili původní primární, než povýšíte sekundární. Pokud má původní primární server stále jinou síťovou konektivitu, máte efektivně spuštěny dvě primární instance současně a data rozdělená na oblasti mohou narůstat. (Pokud odkaz na replikaci funguje, nelze povýšit sekundárního správce front, pokud je primární instance stále spuštěna, příkaz se nezdaří.)
- V uzlu, v němž je spuštěna primární instance správce front, došlo k úplnému selhání sítě. Znovu se musíte ujistit, že zastavíte primární instanci, než povýšíte sekundární instanci. Pokud je předchozí primární server stále spuštěn při obnově sítě, budou existovat dvě primární instance a data rozdělená na oblasti budou opět narůstat.

Při provádění spravovaného překonání selhání byste neměli vidět stav DR `partitioned` pro instance správce front. Spravované překonání selhání ukončí správce front v primárním uzlu a poté spustí správce front v uzlu zotavení po úplné replikaci dat. Stav rozdělený na oblasti není očekáván, protože správce front je ukončen a data jsou synchronizována mezi uzly před jejich spuštěním v uzlu zotavení. Pokud je správce front spuštěn v uzlu zotavení v době, kdy dochází ke ztrátě konektivity mezi uzly, pak je odchylka dat pravděpodobná, pokud byl správce front v hlavním uzlu aktivní, když byla konektivita ztracena. V tomto scénáři se očekává, že po obnovení konektivity bude ohlášen stav rozdělený na oblasti, protože data správce front nebyla synchronizována. Pokud se vyskytne stav rozdělený na oblasti, možná budete muset zkontrolovat tyto dvě datové sady a provést informované rozhodnutí o tom, jakou sadu uchovat. Viz téma “Řešení problému rozděleného na oblasti (rozdělený mozek) v RDQM DR” na stránce 599.

Linux *Požadavky na řešení RDQM DR*

Před konfigurací dvojice správců RDQM pro zotavení z havárie (DR) musíte splnit řadu požadavků.

Systémové požadavky

Před konfigurací RDQM DR musíte provést určitou konfiguraci na každém ze serverů, které mají být hostiteli správců front RDQM DR.

- Každý uzel vyžaduje skupinu disků s názvem `drbdpool`. Úložiště pro každého správce front replikovaných dat pro zotavení z havárie (DR RDQM) je přiděleno jako dva samostatné logické disky pro každého správce front z této skupiny disků. (Každý správce front vyžaduje pro podporu návratu k operaci snímku dva logické disky, takže každý RDQM DR je přidělen těsně nad dvojnásobkem úložiště, které jste zadali při jeho vytvoření.) Pro dosažení nejlepšího výkonu by měla být tato skupina disků tvořena jedním nebo více fyzickými disky, které odpovídají interním diskovým jednotkám (nejlépe SSD).
- Po vytvoření skupiny disků `drbdpool` s ní nic jiného neudělejte. Produkt IBM MQ spravuje logické disky vytvořené v produktu `drbdpool`a způsob a místo jejich připojení.
- Každý uzel vyžaduje rozhraní, které se používá pro replikaci dat. To by mělo mít dostatečnou šířku pásma pro podporu požadavků replikace vzhledem k očekávané pracovní zátěži všech správců front replikovaných dat.

  Pro maximální odolnost proti poruchám by mělo být toto rozhraní nezávislé karty síťového rozhraní (NIC).
- DRBD vyžaduje, aby každý uzel použitý pro RDQM měl platný název hostitele v síti Internet (hodnotu vrácenou produktem `uname -n`), jak je definováno v RFC 952 ve znění RFC 1123.

- Pokud mezi uzly používanými pro RDQM DR existuje brána firewall, musí brána firewall povolit provoz mezi uzly na portech, které se používají pro replikaci. Je poskytnut ukázkový skript `/opt/mqm/samp/rdqm/firewalld/configure.sh`, který otevře nezbytné porty, pokud spouštíte standardní bránu firewall v systému RHEL. Skript musíte spustit jako `root`. Používáte-li jinou bránu firewall, zkontrolujte definice služeb `/usr/lib/firewalld/services/rdqm*` a zjistěte, které porty je třeba otevřít. Skript přidá následující trvalá pravidla služby firewallD pro DRBD a IBM MQ (skript můžete upravit tak, aby vynechaly porty Pacemaker , pokud nepoužíváte HA):
  - MQ_INSTALLATION_PATH/samp/rdqm/firewalld/services/rdqm-drbd.xml umožňuje porty TCP 7000-7100.
  - MQ_INSTALLATION_PATH/samp/rdqm/firewalld/services/rdqm-mq.xml umožňuje port TCP 1414 (skript musíte upravit, pokud požadujete jiný port)
- Pokud systém používá SELinux v jiném než povolujícím režimu, musíte spustit následující příkaz:

```
semanage permissive -a drbd_t
```

Síťové požadavky

Doporučuje se vyhledat uzly použité pro zotavení z havárie v různých datových střediscích.

Měli byste si být vědomi následujících omezení:

- Výkon rychle klesá se zvyšující se latencí mezi datovými středisky. IBM bude podporovat latenci až 5 ms pro synchronní replikaci a 100 ms pro asynchronní replikaci.
- Data odeslaná přes odkaz replikace nepodléhají žádnému dalšímu šifrování kromě toho, které by mohlo být zavedeno z použití IBM MQ AMS.
- Konfigurace správce front RDQM pro zotavení z havárie způsobí režii kvůli požadavku na replikaci dat mezi dvěma uzly RDQM. Synchronní replikace způsobuje vyšší režii než asynchronní replikace. Při použití synchronní replikace jsou operace I/O disku blokovány, dokud se data nezapisují na oba uzly. Při použití asynchronní replikace musí být data zapsána pouze do primárního uzlu, aby mohlo zpracování pokračovat.

Uživatelské požadavky pro práci se správci front

Chcete-li vytvořit, odstranit nebo konfigurovat správce front replikovaných dat (RDQMs), musíte být buď uživatel root, nebo mít ID uživatele patřící do skupiny `mqm` , kterému je uděleno oprávnění sudo pro následující příkazy:

- **`crtmqm`**
- **`dltmqm`**
- **`rdqmdr`**

Uživatel, který patří do skupiny `mqm` , může zobrazit stav RDQM DR pomocí následujících příkazů:

- **`dspmq`**
- **`rdqmstatus`**

Uživatel `mqm` musí mít na obou serverech stejné UID a skupina `mqm` musí mít na obou serverech stejné GID.

Linux *Vytvoření RDQM pro zotavení z havárie*

Pomocí příkazu **`crtmqm`** vytvoříte správce front replikovaných dat (RDQM), který bude fungovat jako primární nebo sekundární v konfiguraci zotavení z havárie.

Informace o této úloze

Můžete vytvořit správce front replikovaných dat (RDQM) jako uživatele ve skupině `mqm` , pokud může uživatel použít příkaz sudo. Jinak musíte vytvořit RDQM jako kořen.

Musíte vytvořit primárního správce front RDQM DR v jednom uzlu. Poté musíte vytvořit sekundární instanci stejného správce front v jiném uzlu. Primární a sekundární instance musí mít stejný název a musí jim být přiděleno stejné množství úložiště.

Následující body poskytují určité vodítko při určování velikosti systému souborů správce front:

1. Při vytváření správce front RDQM je systém souborů přidělen k ukládání dat a protokolů správce front. Je důležité tento systém souborů vhodně nastavit tak, aby mohl správce front zaznamenávat probíhající aktivity do protokolů a ukládat zprávy aplikací do front. Při určování velikosti systému souborů zvažte požadavky na špičkový systém zpráv, budoucí růst pracovní zátěže a výpadky aplikací, které by mohly způsobit sestavení zpráv ve frontách. Informace o výpočtu velikosti protokolu pro zotavení správce front naleznete v části “Jak velký by měl být souborový systém protokolu?” na stránce 632. Při výpočtu požadavků na úložiště pro zprávy aplikace je třeba vzít v úvahu velikost a počet zpráv plus jejich záhlaví MQMD a všechny vlastnosti zpráv, které mají.
2. Velikost systémů souborů správce front RDQM nelze dynamicky měnit. Je-li to vyžadováno, je třeba provést zálohu a poté obnovit správce front RDQM s větším systémem souborů, viz “Změna velikosti systému souborů pro správce front HA RDQM” na stránce 563.
3. Velikost jednotlivých front na disku můžete omezit pomocí atributů lokální fronty, například MAXDEPTH a MAXFSIZE. Viz Úprava IBM MQ.
4. Měli byste monitorovat probíhající využití disku a odpovídajícím způsobem reagovat, pokud se využití disku zvýší dříve, než se využití systému souborů stane kritickým. Využití systému souborů lze monitorovat buď pomocí schopností platformy/operačního systému, nebo přihlášením k odběru metrik publikovaných v tématech systému IBM MQ , která jsou popsána v tématu Metriky publikované v tématech systému.

Procedura

- Chcete-li vytvořit primární RDQM DR, postupujte takto:
  a) Zadejte následující příkaz:

```
crtmqm -rr p [-rt (a | s)] -rl Local_IP -ri Recovery_IP -rn Recovery_Name -rp Port
[other_crtmqm_options] [-fs size] QMname
```

  kde:

  -rr p
  Určuje, že vytváříte primární instanci správce front.

  -rt a | s
  -rt s uvádí, že konfigurace DR používá synchronní replikaci, **-rt a** uvádí, že konfigurace DR používá asynchronní replikaci. Asynchronní replikace je výchozí.

  -rl *Adresa IP lokálního systému*
  Určuje lokální adresu IP, která má být použita pro replikaci DR tohoto správce front.

  -ri *Obnovit_IP*
  Určuje adresu IP rozhraní použitého pro replikaci na serveru, který je hostitelem sekundární instance správce front.

  -rn *Název_obnovení*
  Určuje název systému, který je hostitelem sekundární instance správce front. Název je tato hodnota, která se vrátí, pokud spustíte `uname -n` na tomto serveru. Na tomto serveru musíte explicitně vytvořit sekundárního správce front.

  -rp *Port*
  Určuje port, který má být použit pro replikaci DR.

  další_volení_crtmqm_volby
  Volitelně můžete uvést jednu nebo více z těchto obecných voleb **crtmqm** :

  - `-z`
  - `-q`

- -c *Text*
- -d *DefaultTransmissionFronta*
- -h *MaxHandles*
- -g *ApplicationGroup*
- -oa *uživatel|skupina*
- -t *TrigInt*
- -u *DeadQ*
- -x *MaxUMsgs*
- -lp *LogPri*
- -ls *LogSec*
- -lc | -l
- -lla | -lln
- -lf *LogFile*
- -p *Port*

-fs *velikost*
Volitelně určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického disku vytvořeného ve skupině disků drbdpool. Je také vytvořen další logický disk této velikosti, který podporuje opětovné vrácení na operaci snímku, takže celková paměť pro RDQM DR je téměř dvojnásobná, než je zde uvedeno.

Velikost : Číselná hodnota určená v GB. Hodnotu v MB můžete zadat zadáním hodnoty následované znakem M. Chcete-li například zadat velikost systému souborů 3 GB, zadejte hodnotu 3. Chcete-li určit velikost systému souborů 1024 MB, zadejte hodnotu 1024M. (K explicitnímu stavu GB můžete také přidat příponu G.)

QMNAME
Určuje název správce front replikovaných dat. V názvu jsou rozlišována velká a malá písmena.

Po dokončení příkazu je výstupem příkazu, který je třeba zadat do sekundárního uzlu, aby se vytvořila sekundární instance správce front. Můžete také použít příkaz **rdqmdr** na primárním uzlu k načtení příkazu **crtmqm** , který musíte spustit na sekundárním uzlu, abyste vytvořili sekundárního správce front, viz "Správa primárních a sekundárních charakteristik RDQM DR" na stránce 590.

- Chcete-li vytvořit sekundární RDQM DR, postupujte takto:

a) Zadejte následující příkaz na uzlu, který má být hostitelem sekundárních instancí RDQM:

```
crtmqm  -rr s [-rt (a | s)] -rl Local_IP -ri Primary_IP -rn Primary_Name  -rp Port
[other_crtmqm_options] [-fs size] QMname
```

Kde:

-rr s
Určuje, že vytváříte sekundární instanci správce front.

-rt a | s
-rt s uvádí, že konfigurace DR používá synchronní replikaci, **-rt a** uvádí, že konfigurace DR používá asynchronní replikaci.

-rl *Adresa IP lokálního systému*
Určuje lokální adresu IP, která má být použita pro replikaci DR tohoto správce front.

-ri *Primární_IP*
Určuje adresu IP rozhraní použitého pro replikaci na serveru, který je hostitelem primární instance správce front.

-rn *Primary_Name*
Určuje název systému, který je hostitelem primární instance správce front. Název je tato hodnota, která se vrátí, pokud spustíte uname -n na tomto serveru.

-rp ***Port***
Určuje port, který má být použit pro replikaci DR.

další_volení_crtmqm_volby
Volitelně můžete uvést jednu nebo více z těchto obecných voleb **crtmqm** :

– -z

-fs ***velikost***
Určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického disku vytvořeného ve skupině disků drbdpool. Pokud jste při vytváření primárního správce front zadali jinou než výchozí velikost, musíte zde zadat stejnou hodnotu.

Velikost : Číselná hodnota určená v GB. Hodnotu v MB můžete zadat zadáním hodnoty následované znakem M. Chcete-li například zadat velikost systému souborů 3 GB, zadejte hodnotu 3. Chcete-li určit velikost systému souborů 1024 MB, zadejte hodnotu 1024M. (K explicitnímu stavu GB můžete také přidat příponu G.)

QMNAME
Určuje název správce front replikovaných dat. Musí se shodovat s názvem, který jste zadali pro primární instanci správce front. Všimněte si, že název rozlišuje malá a velká písmena.

Jak pokračovat dále

Po vytvoření primární a sekundární instance správce front musíte zkontrolovat stav na obou uzlech, abyste zkontrolovali, zda jsou obě správné. Použijte příkaz **rdqmstatus** na obou uzlech. Uzly by měly zobrazovat normální stav, jak je popsáno v tématu “Zobrazení stavu RDQM DR” na stránce 592. Pokud tento stav nezobrazují, odstraňte sekundární instanci a znovu ji vytvořte s ohledem na použití správných argumentů.

Související odkazy

crtmqm

Linux *Odstranění RDQM DR*

Pomocí příkazu **dltmqm** můžete odstranit správce front replikovaných dat pro zotavení z havárie (RDQM).

Informace o této úloze

Musíte spustit příkaz k odstranění RDQM na primárním i sekundárním uzlu RDQM. Nejprve musí být ukončen RDQM. Příkaz můžete spustit jako uživatel mqm, pokud má tento uživatel nezbytná oprávnění k příkazu sudo. Jinak musíte příkaz spustit jako uživatel root.

Procedura

- Chcete-li odstranit RDQM DR, zadejte následující příkaz:

```
dltmqm RDQM_name
```

Související odkazy

dltmqm

Linux MQ Adv. *Migrace správce front na správce front DR RDQM*

Můžete migrovat existujícího správce front tak, aby se stal správcem front replikovaných dat zotavení z havárie (RDQM), a to tak, že zálohujete jeho trvalá data a poté data obnovíte do nově vytvořeného správce front RDQM se stejným názvem.

Informace o této úloze

Správci front replikovaných dat DR vyžadují vyhrazený logický svazek (systém souborů) a konfiguraci replikace disku. Tyto komponenty jsou konfigurovány pouze při vytvoření nového správce front. Existujícího správce front lze migrovat pro použití RDQM zálohováním jeho trvalých dat a následným obnovením dat do nově vytvořeného správce front RDQM se stejným názvem. Tento postup zachovává konfiguraci, stav a trvalé zprávy správce front v době vytvoření zálohy.

Poznámka: Správce front lze migrovat pouze z verze produktu IBM MQ , která je stejná nebo nižší než verze, ve které je nainstalován produkt RDQM. Operační systém a architektura musí být stejné. Jinak musíte na cílové platformě vytvořit nového správce front. Viz téma Přesunutí správce front do jiného operačního systému.

Před migrací správce front byste měli splňovat následující podmínky:

- Vyhodnoťte své požadavky na zotavení z havárie a prohlédněte si téma “Zotavení z havárie RDQM” na stránce 577.
- Zkontrolujte aplikace a správce front, kteří se připojují ke správci front. Zvažte změny nezbytné pro směrování připojení do uzlu RDQM, kde je spuštěn správce front.
- Zajistěte nebo identifikujte existující uzly RDQM pro zvolenou konfiguraci. Informace o systémových požadavcích RDQM viz “Požadavky na řešení RDQM DR” na stránce 580.
- Nainstalujte produkt IBM MQ Advanced, který zahrnuje funkci RDQM, na každý uzel.
- Volitelně ověřte konfiguraci RDQM pomocí správce front testu, který lze poté odstranit. Testování konfigurace se doporučuje k identifikaci a vyřešení případných problémů před migrací správce front.
- Zkontrolujte konfiguraci zabezpečení pro správce front a poté proveďte replikaci požadovaných lokálních uživatelů a skupin v jednotlivých uzlech RDQM.
- Zkontrolujte konfiguraci správce front a kanálu a určete, zda jsou použity uživatelské procedury rozhraní API, uživatelské procedury kanálu nebo uživatelské procedury pro převod dat. Nainstalujte požadované uživatelské procedury na každý uzel RDQM.
- Zkontrolujte všechny definované služby správce front a poté nainstalujte a nakonfigurujte požadované procesy v každém uzlu RDQM.

Postup

1. Zazálohujte existujícího správce front:
   a) Zastavte existujícího správce front zadáním příkazu wait shutdown `endmqm -w`nebo příkazu immediate shutdown `endmqm -i`. Tento krok je důležitý pro zajištění konzistence dat v záloze.
   b) Určete umístění datového adresáře správce front zobrazením konfiguračního souboru IBM MQ `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`viz “IBM MQ konfigurační soubor mqs.ini” na stránce 85.

      Vyhledejte sekci `QueueManager` pro správce front v souboru. Pokud sekce obsahuje klíč s názvem `DataPath` , její hodnota je datový adresář správce front. Pokud klíč neexistuje, lze datový adresář správce front určit pomocí hodnot klíčů `Prefix` a `Directory` . Datový adresář správce front je zřetězením těchto hodnot ve tvaru *předpona*/qmgrs/*adresář*. Další informace o sekci QueueManager naleznete v části “QueueManager sekce souboru mqs.ini” na stránce 95.
   c) Vytvořte zálohu datového adresáře správce front. V systému Linuxto můžete provést pomocí příkazu **`tar`** . Chcete-li například zálohovat datový adresář pro správce front, můžete použít následující příkaz. Všimněte si posledního parametru příkazu, kterým je jedna tečka (tečka):

      ```
      tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
      ```

   d) Určete umístění adresáře protokolu správce front zobrazením IBM MQ konfiguračního souboru správce front `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front, qm.ini” na stránce 97.

      Adresář protokolu správce front je definován jako hodnota klíče `LogPath` v sekci `Log` . Informace o sekci viz “Sekce protokolu souboru qm.ini” na stránce 130.
   e) Vytvořte zálohu adresáře protokolu správce front. V systému Linuxto můžete provést pomocí příkazu tar. Chcete-li například zálohovat adresář protokolu pro správce front, můžete použít následující příkaz. Všimněte si posledního parametru příkazu, kterým je jedna tečka (tečka):

      ```
      tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
      ```

f) Vytvořte zálohu všech úložišť certifikátů používaných správcem front, pokud nejsou umístěna v datovém adresáři správce front. Ujistěte se, že je zálohován soubor databáze klíčů i soubor pro uložení hesla. Informace o úložišti klíčů správce front naleznete v tématu Úložiště klíčů SSL/TLS a Vyhledání úložiště klíčů pro správce front. Informace o vyhledání úložiště klíčů AMS v případě, že je správce front konfigurován pro použití zachycení agenta MCA (AMS Message Channel Agent), naleznete v tématu Zachycení agenta MCA (Message Channel Agent).

g) Existující správce front již není vyžadován, takže jej lze odstranit. Pokud je to však možné, měli byste odstranit existujícího správce front pouze po jeho úspěšném obnovení v cílovém systému. Odložení odstranění zajistí, že správce front bude možné restartovat, pokud se proces migrace nedokončí úspěšně.

Poznámka: Pokud odložíte odstranění existujícího správce front, nerestartujte jej. Je důležité, aby správce front zůstal ukončen, protože během migrace dojde ke ztrátě dalších změn jeho konfigurace nebo stavu.

2. Připravte primární uzel RDQM:

a) Vytvořte nového správce front RDQM se stejným názvem jako zálohovaný správce front. Ujistěte se, že systém souborů přidělený pro správce front RDQM produktem **crtmqm** je dostatečně velký na to, aby obsahoval data, primární protokoly a sekundární protokoly pro existujícího správce front, plus další prostor pro budoucí rozšíření. Informace o vytvoření správce front RDQM viz "Vytvoření RDQM pro zotavení z havárie" na stránce 581.

b) Určete primární uzel RDQM pro správce front. Informace o tom, jak určit primární uzel, viz rdqmstatus (zobrazení stavu RDQM).

c) Pokud je v primárním uzlu RDQM spuštěn správce front RDQM, zastavte jej pomocí příkazu `endmqm -w` nebo `endmqm -i` .

d) Určete umístění adresářů dat a protokolů pro správce front RDQM (použijte metody popsané v krocích 1b a 1d).

e) Odstraňte obsah datových a protokolovacích adresářů správce front RDQM, nikoli však samotných adresářů.

3. Obnovte správce front v primárním uzlu RDQM:

a) Zkopírujte zálohy dat a adresářů protokolů správce front do primárního uzlu RDQM a dále všechny samostatné zálohy úložišť certifikátů používaných správcem front.

b) Obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a zajistěte zachování vlastnictví souborů a oprávnění. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1c , uživatel root může k její obnově použít následující příkaz:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

c) Obnovte zálohu adresáře protokolu správce front do prázdného adresáře protokolu pro nového správce front RDQM, čímž zajistíte zachování vlastnictví souboru a oprávnění. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1e , uživatel root může k její obnově použít následující příkaz:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

d) Upravte obnovený konfigurační soubor správce front `qm.ini`v datovém adresáři pro správce front RDQM. Aktualizujte hodnotu klíče `LogPath` v sekci `Log` tak, aby uváděla adresář protokolu pro správce front RDQM.

Přezkoumejte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Můžete například potřebovat aktualizovat následující cesty:

- Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
- Cesta pro uživatelské procedury, které jsou vyžadovány správcem front.
- Cesta k souborům načtení přepínače, pokud je správcem front koordinátor transakcí XA.

e) Je-li správce front konfigurován tak, aby používal zachytávání agenta MCA (AMS Message Channel Agent), zkopírujte úložiště klíčů AMS do nové instalace RDQM a poté zkontrolujte a aktualizujte konfiguraci. Úložiště klíčů musí být k dispozici v každém uzlu RDQM, takže pokud není umístěno v replikovaném systému souborů pro správce front, musí být zkopírováno do každého uzlu. Další informace naleznete v tématu Zachycení agenta MCA (Message Channel Agent).

f) Ověřte, že je správce front zobrazen příkazem **dspmq** a jeho stav je ohlášen jako ukončený. Následující příklad ukazuje ukázku výstupu pro správce front RDQM DR:

```
$ dspmq -o status -o dr

QMNAME(QM1) STATUS(Ended normally) DRROLE(Primary)
```

g) Pomocí příkazu **rdqmstatus** ověřte, zda byla obnovená data správce front replikována do sekundárních uzlů RDQM, a zobrazte tak stav správce front. Stav DR by měl být na každém uzlu vykazován jako `Normal` . Následující příklad ukazuje ukázku výstupu pro správce front RDQM DR:

```
$ rdqmstatus -m QM1
Queue manager status:                   Ended normally
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Normal
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
```

h) Spusťte správce front v primárním uzlu RDQM.

i) Připojte se ke správci front a aktualizujte hodnotu atributu správce front SSLKEYR tak, aby určovala nové umístění úložiště certifikátů správce front. Standardně je hodnota tohoto atributu nastavena na *queue_manager_data_directory*`/ssl/key`. Úložiště certifikátů musí být umístěno ve stejném umístění na každém uzlu RDQM. Pokud se úložiště nenachází v replikovaném systému souborů pro správce front, musí být zkopírováno do každého uzlu.

j) Zkontrolujte definice objektů IBM MQ pro správce front a aktualizujte hodnotu atributů objektů, které odkazují na změněná nastavení sítě, instalační adresář produktu IBM MQ nebo datový adresář správce front, včetně následujících objektů:

- Lokální adresy IP používané listenery (atribut`IPADDR`).
- Lokální adresy IP používané kanály (atribut`LOCLADDR`).
- Lokální adresy IP definované pro přijímací kanály klastru (atribut`CONNAME`).
- Lokální adresy IP definované pro objekty informací o komunikaci (atribut`GRPADDR`).
- Systémové cesty definované pro definice objektů procesů a služeb.

k) Zastavte a restartujte správce front, aby se změny projevily.

l) Zopakujte krok 3j pro vzdálené správce front a ekvivalentní nastavení pro aplikace, které se připojují k migrovanému správci front, včetně:

- Názvy připojení kanálu (atribut`CONNAME`).
- Pravidla ověřování kanálu, která omezují příchozí připojení ze správce front na základě adresy IP nebo názvu hostitele.
- Tabulky CCDT (Client Channel Definition Table), DNS (Domain Name settings), směrování v síti nebo ekvivalentní informace o připojení.

m) Proveďte spravované překonání selhání správce front pro každý uzel RDQM, abyste se ujistili, že požadovaná konfigurace byla úspěšně vytvořena, viz “Přepnutí na uzel obnovy” na stránce 596.

Změna velikosti systému souborů pro správce front RDQM DR
Chcete-li změnit velikost souborového systému pro existujícího správce front replikovaných dat zotavení z havárie (RDQM), který zálohujete jeho trvalá data, obnovte data do nově vytvořeného správce front RDQM, který má stejný název, ale jinou velikost systému souborů.

Informace o této úloze

Správci front replikovaných dat DR vyžadují vyhrazený logický svazek (systém souborů) a konfiguraci replikace disku. Tyto komponenty jsou konfigurovány pouze při vytvoření nového správce front. Po vytvoření systému souborů nelze změnit jeho velikost, protože musí mít na každém uzlu stejnou velikost. Chcete-li změnit velikost systému souborů pro existujícího správce front replikovaných dat (RDQM), můžete zálohovat jeho trvalá data a poté obnovit data do nově vytvořeného správce front RDQM, který má stejný název, ale jiný systém souborů jiné velikosti. Tento postup zachovává konfiguraci, stav a trvalé zprávy správce front v době vytvoření zálohy.

Postup

1. Zazálohujte existujícího správce front RDQM na primárním uzlu RDQM:
   a) Určete primární uzel RDQM pro správce front. Informace o tom, jak určit primární uzel, viz rdqmstatus (zobrazení stavu RDQM) .
   b) Pokud je v primárním uzlu RDQM spuštěn správce front RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .
   c) Určete umístění datového adresáře správce front zobrazením konfiguračního souboru IBM MQ `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`viz “IBM MQ konfigurační soubor mqs.ini” na stránce 85.

      Vyhledejte sekci `QueueManager` pro správce front v souboru. Datový adresář správce front je hodnota klíče s názvem `DataPath`. Další informace o sekci `QueueManager` viz “QueueManager sekce souboru mqs.ini” na stránce 95.
   d) Vytvořte zálohu datového adresáře správce front. V systému Linuxto můžete provést pomocí příkazu **tar** . Chcete-li například zálohovat datový adresář pro správce front, můžete použít následující příkaz. Povšimněte si posledního parametru příkazu, který je jedním znakem tečky (.):

      ```
      tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
      ```
   e) Určete umístění adresáře protokolu správce front zobrazením IBM MQ konfiguračního souboru správce front `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front, qm.ini” na stránce 97.

      Adresář protokolu správce front je definován jako hodnota klíče `LogPath` v sekci Protokol. Informace o sekci viz “Sekce protokolu souboru qm.ini” na stránce 130.
   f) Vytvořte zálohu adresáře protokolu správce front. V systému Linuxto můžete provést pomocí příkazu **tar** . Chcete-li například zálohovat adresář protokolu pro správce front, můžete použít následující příkaz. Povšimněte si posledního parametru příkazu, který je jedním znakem tečky (.):

      ```
      tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
      ```
   g) Odstraňte existujícího správce front RDQM.
2. Obnovte správce front s požadovaným systémem souborů:
   a) Vytvořte nového správce front RDQM se stejným názvem jako zálohovaný správce front. Ujistěte se, že systém souborů přidělený pro správce front RDQM produktem **crtmqm** má požadovanou velikost a že je dostatečně velký na to, aby obsahoval data, primární protokoly a sekundární protokoly pro existujícího správce front, plus další prostor pro budoucí rozšíření. Informace o vytvoření správce front RDQM viz “Vytvoření RDQM pro zotavení z havárie” na stránce 581.
   b) Určete primární uzel RDQM pro správce front. Informace o tom, jak určit primární uzel, viz rdqmstatus (zobrazení stavu RDQM).
   c) Pokud je v primárním uzlu RDQM spuštěn správce front RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .
   d) V primárním uzlu RDQM určete nové umístění adresářů dat a protokolů pro správce front RDQM (použijte metody popsané v krocích 1c a 1e).

e) V primárním uzlu RDQM odstraňte obsah dat a adresářů protokolu správce front RDQM, nikoli však samotné adresáře.

f) V primárním uzlu RDQM obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a zajistěte zachování vlastnictví souboru a oprávnění. Pokud byla záloha vytvořena pomocí příkladu příkazu **tar** v kroku 1d , může uživatel root k její obnově použít následující příkaz:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

g) V primárním uzlu RDQM obnovte zálohu adresáře protokolu správce front do prázdného adresáře protokolu pro nového správce front RDQM a zajistěte zachování vlastnictví souborů a oprávnění. Pokud byla záloha vytvořena pomocí příkladu příkazu **tar** v kroku 1f , může uživatel root k její obnově použít následující příkaz:

```
tar -xvzpf qm-log.tar.gz -C queue_manager_log_dir
```

h) V primárním uzlu RDQM upravte obnovený konfigurační soubor správce front `qm.ini` v datovém adresáři pro nového správce front RDQM. Aktualizujte hodnotu klíče `LogPath` v sekci `Log` tak, aby uváděla adresář protokolu pro nového správce front RDQM, kterého jste určili v kroku 2d. Přezkoumejte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Můžete například potřebovat aktualizovat následující cesty:

- Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
- Cesta pro uživatelské procedury, které jsou vyžadovány správcem front.
- Cesta k souborům načtení přepínače, pokud je správcem front koordinátor transakcí XA.

i) Ověřte, že je správce front zobrazen příkazem **dspmq** a jeho stav je ohlášen jako `ended`. Následující příklad ukazuje ukázku výstupu pro správce front RDQM DR:

```
$ dspmq -o status -o dr
QMNAME(QM1) STATUS(Ended normally) DR(Primary)
```

j) Pomocí příkazu **rdqmstatus** ověřte, že obnovená data správce front byla replikována do sekundárního uzlu RDQM, aby se zobrazil stav správce front. Stav DR by měl být na každém uzlu vykazován jako `Normal` . Následující příklad ukazuje ukázku výstupu pro správce front RDQM DR v primárním uzlu:

```
$ rdqmstatus -m QM1
Queue manager status:                 Running
CPU:                                  0.00
Memory:                               123MB
Queue manager file system:            51MB used, 1.0GB allocated [5%]
DR role:                              Primary
DR status:                            Normal
DR type:                              Synchronous
DR port:                              3000
DR local IP address:                  192.168.20.1
DR remote IP address:                 192.168.20.2
```

Následující příklad ukazuje ukázku výstupu pro správce front RDQM DR v uzlu zotavení:

```
Queue manager status:                 Ended immediately
DR role:                              Secondary
DR status:                            Normal
DR port:                              3000
DR local IP address:                  192.168.20.2
DR remote IP address:                 192.168.20.1
```

k) Spusťte správce front v primárním uzlu RDQM.

l) Proveďte přepnutí správce front do uzlu zotavení, abyste se ujistili, že požadovaná konfigurace byla úspěšně vytvořena, viz “Přepnutí na uzel obnovy” na stránce 596.

Ukládání stavu trvalé aplikace

Můžete uložit informace o trvalém stavu týkající se aplikací spolu s dalšími daty správce front.

Každý správce front IBM MQ má vyhrazený systém souborů pro svůj trvalý stav, který zahrnuje jak data fronty, tak protokol zotavení. V konfiguraci RDQM je systém souborů zálohován logickým svazkem, který je replikován mezi systémy Linux (uzly). Systém souborů obsahuje adresář `userdata` , který můžete použít k uložení informací o trvalém stavu pro vaše aplikace. Takže když se správce front replikovaných dat přesune ke spuštění v jiném uzlu v konfiguraci RDQM, máte k dispozici kontext aplikace i kontext správce front. Viz Obsah adresáře v systémech Unix a Linux Systems.

Pokud se rozhodnete uložit stav aplikace do adresáře `userdata` , musíte si uvědomit, že data zapsaná do tohoto umístění mohou spotřebovat dostupné místo na disku přidělené správci front. Je třeba zajistit, aby byl pro správce front k dispozici dostatek místa na disku pro zápis dat fronty, protokolů a dalších informací o trvalém stavu.

Adresář `userdata` má vlastnictví uživatele mqm a skupiny a je čitelný, takže k němu mohou uživatelé přistupovat, aniž by museli být ve skupině administrátorů IBM MQ (tj. mqm). Nemůžete upravit oprávnění adresáře `userdata` , ale můžete v něm vytvořit obsah s libovolným vlastnictvím a oprávněními, která požadujete.

Během překonání selhání správce front RDQM je správce front ukončen a jeho systém souborů je odpojen od aktuálního uzlu RDQM. Systém souborů je poté připojen a správce front je restartován v jiném uzlu v konfiguraci RDQM. Systém souborů nelze odpojit, pokud má proces otevřený popisovač pro jeden ze svých souborů. Chcete-li zajistit dokončení překonání selhání správce front, v případě, že systém souborů správce front nelze odpojit, budou procesům s otevřenou manipulací se odešle signál SIGTERM následovaný signálem SIGKILL, nejsou-li otevřené manipulátory uvolněny. Vaše aplikace musí být navrženy tak, aby správně reagovaly na SIGTERM. Jsou-li aplikace nebo procesy konfigurovány jako služba správce front, mohou být během spravovaného překonání selhání ukončeny během ukončování činnosti správce front před odpojením systému souborů. Pokud aplikace nebo proces není konfigurován jako služba správce front nebo dojde k nespravovanému překonání selhání, například ke ztrátě kvora, pak je pravděpodobné, že budou odeslány signály pro uvolnění systému souborů.

Linux *Správa primárních a sekundárních charakteristik RDQM DR*

Můžete změnit sekundární správce front replikovaných dat pro zotavení z havárie (DR RDQM) na primární RDQM DR. Můžete také změnit primární instanci na sekundární instanci.

Informace o této úloze

Pomocí příkazu **rdqmdr** změníte sekundární instanci RDQM na primární instanci. Možná budete muset dokončit tuto akci, pokud z nějakého důvodu ztratíte primární instanci. Poté můžete spustit správce front a pokračovat v jeho spouštění v uzlu zotavení.

Pomocí příkazu **rdqmdr** můžete také změnit primární instanci RDQM na sekundární instanci. Možná budete muset dokončit tuto akci, například pokud jste překonfigurovali systém.

Můžete také použít **rdqmdr** v primárním správci front k načtení přesného příkazu, který potřebujete k vytvoření sekundární instance tohoto správce front v uzlu zotavení.

Příkaz **rdqmdr** můžete použít jako uživatele ve skupině `mqm` , pokud může uživatel použít příkaz sudo. Jinak musíte být přihlášeni jako uživatel root.

Procedura

- Chcete-li změnit sekundární instanci RDQM DR na primární instanci, zadejte následující příkaz:

  ```
  rdqmdr -m QMname -p
  ```

  Tento příkaz selže, pokud je primární instance správce front stále spuštěna a odkaz na replikaci DR stále funguje.
- Chcete-li změnit primární instanci správce front na sekundární instanci, zadejte následující příkaz:

  ```
  rdqmdr -m QMname -s
  ```

- Chcete-li zobrazit příkaz **crtmqm** nezbytný ke konfiguraci sekundární instance správce front, zadejte na primárním uzlu následující příkaz:

  ```
  rdqmdr -d -m QMname
  ```

  Můžete zadat vrácený příkaz **crtmqm** ve svém sekundárním uzlu a vytvořit sekundární instanci RDQM RD.

Linux *Spuštění, zastavení a zobrazení stavu RDQM DR*

Varianty standardních řídicích příkazů IBM MQ se používají ke spuštění, zastavení a zobrazení aktuálního stavu správce front replikovaných dat zotavení z havárie (DR RDQM).

Informace o této úloze

Musíte spustit příkazy, které spustí, zastaví a zobrazí aktuální stav správce front replikovaných dat (RDQM) jako uživatel, který patří do skupiny `mqm` .

Je třeba spustit příkazy pro spuštění a zastavení správce front v primárním uzlu pro daného správce front (tj. v uzlu, v němž je správce front aktuálně spuštěn).

Procedura

- Chcete-li spustit RDQM DR, zadejte na primárním uzlu RDQM následující příkaz:

  ```
  strmqm qmname
  ```

  kde *qmname* je název RDQM, který chcete spustit.
- Chcete-li zastavit RDQM, zadejte na primárním uzlu RDQM následující příkaz:

  ```
  endmqm qmname
  ```

  kde *qmname* je název RDQM, který chcete zastavit.
- Chcete-li zobrazit stav RDQM, zadejte následující příkaz:

  ```
  dspmq -m QMname
  ```

  Výstupní informace o stavu závisí na tom, zda jste spustili příkaz na primárním nebo sekundárním uzlu RDQM. Pokud se spustí na primárním uzlu, zobrazí se jedna z běžných stavových zpráv vrácených produktem **dspmq** . Spustíte-li příkaz na sekundárním uzlu, zobrazí se stav `Ended immediately` . Pokud je například produkt **dspmq** spuštěn na uzlu RDQM7, mohou být vráceny následující informace:

  ```
  QMNAME(DRQM8)                           STATUS(Ended immediately)
  QMNAME(DRQM7)                           STATUS(Running)
  ```

  Pomocí argumentů s produktem `dspmq` můžete určit, zda je RDQM konfigurován pro zotavení z havárie a zda je momentálně primární nebo sekundární instancí:

  ```
  dspmq -m QMname -o (dr | DR)
  ```

  Zobrazí se jedna z následujících odpovědí:

  DRROLE()
  Označuje, že správce front není konfigurován pro zotavení z havárie.

  DRROLE(Primary)
  Označuje, že je správce front konfigurován jako primární DR.

  DRROLE(Secondary)
  Označuje, že správce front je konfigurován jako sekundární DR.

Související odkazy

-živec

endmqm
strmqm

Linux *Zobrazení stavu RDQM DR*

Můžete zobrazit stav všech správců front replikovaných dat zotavení z havárie (DR RDQMs) v uzlu nebo podrobné informace pro určený RDQM DR.

Informace o této úloze

Příkaz **rdqmstatus** použijte k zobrazení stavu všech RDQM DR nebo jednotlivých RDQM.

V 9.3.0 Souhrnný stav uzlu také zobrazuje informace o modulu jádra DRBD, na kterém RDQM spoléhá. Při upgradu RDQM je důležité zajistit, aby byla pro verzi jádra RHEL spuštěného v systému nainstalována správná verze modulu jádra DRBD. Stav zobrazuje verzi jádra operačního systému, verzi jádra, pro kterou byl modul DRBD sestaven, verzi DRBD a stav načtení modulu jádra DRBD.

Chcete-li spustit příkaz **rdqmstatus** , musíte být uživatel ve skupině `mqm` . Příkaz můžete spustit na kterémkoli uzlu dvojice RDQM DR.

Procedura

- Chcete-li zobrazit souhrnný stav všech RDQM DR na uzlu, spusťte na tomto uzlu následující příkaz:

  ```
  rdqmstatus
  ```

  Zobrazí se stav RDQM DR na uzlu, například:

  ```
  Node:                                mqhavm07.exampleco.com
  OS kernel version:                   3.10.0-1160.15.2
  DRBD OS kernel version:              3.10.0-1160
  DRBD version:                        9.1.1
  DRBD kernel module status:           Loaded

  Queue manager name:                  DRQM8
  Queue manager status:                Ended immediately
  DR role:                             Secondary

  Queue manager name:                  DRQM7
  Queue manager status:                Running
  DR role:                             Primary
  ```

  V 9.3.0 Stav modulu jádra DRBD je jedna z následujících hodnot:

  Načteno
  Označuje, že byl načten modul DRBD.

  Částečně načteno
  Může se vyskytnout, když byl modul DRBD načten, ale nefunguje správně kvůli neshodě.

  Nenačteno

  Modul DRBD není načten. Tuto možnost lze zobrazit v nově nainstalované konfiguraci v případě, že dosud nebyli vytvořeni žádní správci front RDQM.

  Neinstalováno
  Označuje, že buď modul DRBD není nainstalován. nebo že produkt IBM MQ nemohl určit verzi jádra operačního systému modulu DRBD.

  Dříve nainstalovaná verze je stále načtena
  Tento stav může nastat, pokud je nainstalován nový modul DRBD, zatímco je spuštěn existující modul DRBD (tj. je spuštěn správce front RDQM). Nově nainstalovaný modul je ohlášen ve stavu, ale nejedná se o modul, který je ve skutečnosti spuštěn.

- Chcete-li zobrazit stav konkrétního RDQM, zadejte následující příkaz:

  ```
  rdqmstatus -m  qmname
  ```

Následující tabulka shrnuje vrácené informace.

Tabulka 34. Atributy stavu

Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Stav správce front	stav (jak zobrazuje `dspmq`)	Vždy zobrazeno
CPU	*n.nn*%	Zobrazeno pouze v případě, že má RDQM na aktuálním uzlu primární roli
Paměť	*nnn*MB	Zobrazeno pouze v případě, že má RDQM na aktuálním uzlu primární roli
Systém souborů správce front	*nnn*použité MB*, n.n*přidělené GB [*n*%]	Zobrazeno pouze v případě, že má RDQM na aktuálním uzlu primární roli
Role DR	Primární Sekundární Neznámý	Vždy zobrazeno
Stav DR	Normální	Normální provoz
	Probíhá synchronizace	Probíhá synchronizace
	Rozděleno na oblasti	Správce front byl spuštěn na obou uzlech, zatímco replikační síť DR není k dispozici.
	Vzdálený systém není k dispozici	Připojení k jinému uzlu bylo ztraceno
	Nekonzistentní	Synchronizace probíhala, ale byla přerušena
	Návrat na snímek	Uživatel se rozhodl vrátit se ke snímku, který byl pořízen, když správce front přešel do nekonzistentního stavu.
	Vzdálený systém není nakonfigurován	Primární instance RDQM byla konfigurována, ale nebyla konfigurována žádná sekundární instance.
	Nezdařená vyjednávání	Jeden z uzlů byl nastaven na synchronní replikaci a druhý na asynchronní replikaci.
Typ DR	Synchronní nebo asynchronní	Vždy zobrazeno
Port DR	*číslo_portu* (port TCP/IP použitý k replikaci dat pro tohoto správce front)	Vždy zobrazeno
Lokální adresa IP DR	Lokální adresa IP, ze které se tento správce front replikuje pro DR	Vždy zobrazeno

Tabulka 34. Atributy stavu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Vzdálená IP adresa DR	Adresa IP vzdáleného systému, na kterou se tento správce front replikuje pro DR	Vždy zobrazeno
Nesynchronizovaná data DR	*n*KB	Zobrazí se, když je vzdálený uzel nedostupný nebo nekonzistentní
Průběh synchronizace DR	*n*%	Zobrazí se, když probíhá synchronizace
Předpokládaný čas dokončení DR	*RRRR-MM-DD HH*:*MM*:*SS*	Zobrazí se, když probíhá synchronizace
Průběh opětovného vrácení snímku	*n*%	Zobrazí se, když je stav DR `Reverting to snapshot`. Stav se počítá dolů, takže 0% zobrazuje dokončení
V 9.3.0 V 9.3.0 DR naposledy synchronizováno	*RRRR-MM-DD HH*:*MM*:*SS*	Zobrazí se, když jsou data DR nesynchronizovaná (po počáteční synchronizaci). Udává čas a datum, kdy byla data naposledy synchronizována.

Příklad

Příklad normálního stavu na primárním uzlu:

```
Queue manager status:                   Running
CPU:                                    0.00
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Normal
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
```

Příklad normálního stavu na sekundárním uzlu:

```
Queue manager status:                   Ended immediately
DR role:                                Secondary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.20.2
DR remote IP address:                   192.168.20.1
```

Příklad stavu na primárním uzlu při probíhající synchronizaci:

```
Queue manager status:                   Running
CPU:                                    0.53
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Synchronization in progress
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
DR synchronization progress:            11.0%
DR estimated time to completion:        2017-09-06 14:55:05
```

Příklad primárního uzlu, který ukazuje, že je rozdělený na oblasti:

```
Queue manager status:                   Running
CPU:                                    0.02
Memory:                                 124MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Partitioned
DR type:                                Synchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
```

V 9.3.0 Příklad primárního uzlu, který ukazuje, že není synchronizován se sekundárním uzlem:

```
Queue manager status:                   Running
CPU:                                    0.00
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
DR role:                                Primary
DR status:                              Remote unavailable
DR type:                                Asynchronous
DR port:                                3000
DR local IP address:                    192.168.20.1
DR remote IP address:                   192.168.20.2
DR out of sync data:                    15932KB
DR last in sync:                        2020-07-27 16:01:47
```

V 9.3.0 Příklad souhrnného stavu, který ukazuje neshodu mezi verzí jádra operačního systému (RHEL 7.9) a modulem jádra DRBD (zaměřeno na RHEL 7.8). Přestože jsou zprávy o stavu, že modul jádra DRBD je načten a je spuštěn očekávaný správce front, měli byste modul jádra DRBD aktualizovat na verzi, která je v této situaci určena pro spuštěné jádro operačního systému.

```
Node:                                   mqhavm07.exampleco.com
OS kernel version:                      3.10.0-1160.15.2
DRBD OS kernel version:                 3.10.0-1127
DRBD version:                           9.1.1
DRBD kernel module status:              Loaded

Queue manager name:                     DRQM8
Queue manager status:                   Ended immediately
DR role:                                Secondary

Queue manager name:                     DRQM7
Queue manager status:                   Running
DR role:                                Primary
```

V 9.3.0 Příklad souhrnného stavu ukazujícího neshodu mezi verzí jádra operačního systému (RHEL 7.9) a modulem jádra DRBD (zaměřeným na RHEL 7.6). V tomto příkladu je neshoda verzí závažnější a modul jádra DRBD se nepodařilo úspěšně načíst. QM3 je správce front DR a je určen jako primární instance, ale vzhledem k tomu, že modul jádra DRBD nebyl plně načten, hlásí se jako sekundární se stavem DR Unknown. Chcete-li toto selhání vyřešit, musí být modul jádra DRBD aktualizován s cílem verze pro spuštěné jádro operačního systému.

```
Node:                                   mqhavm57.exampleco.com
OS kernel version:                      3.10.0-1160.15.2
DRBD OS kernel version:                 3.10.0-957
DRBD version:                           9.1.2+ptf.3
DRBD kernel module status:              Partially loaded

Queue manager name:                     QM3
Queue manager status:                   Status not available
DR role:                                Secondary
DR status:                              Unknown
```

Související odkazy

Linux rdqmstatus

Linux *Provoz v prostředí zotavení z havárie*

Může se stát, že v konfiguraci zotavení z havárie budete chtít přepnout na sekundárního správce front.

Zotavení z havárie
Po úplné ztrátě primárního správce front na hlavním serveru spustíte sekundárního správce front na serveru pro zotavení. Aplikace se znovu připojí ke správci front na serveru pro zotavení a sekundární správce front zpracuje zprávy aplikací. Kroky, které se mají vrátit k předchozí konfiguraci, závisí na příčině selhání. Například úplná ztráta hlavního uzlu versus dočasná ztráta.

Kroky, které je třeba provést po dočasné ztrátě hlavního serveru, viz "Přepnutí na uzel obnovy" na stránce 596. Postup při následování trvalého selhání naleznete v části "Nahrazení uzlu, který selhal, v konfiguraci zotavení z havárie" na stránce 597.

Podpora testu zotavení z havárie
Konfiguraci zotavení z havárie můžete otestovat dočasným přepnutím na sekundární instanci a kontrolou, zda se aplikace mohou úspěšně připojit. Postupujte stejně, jako když přepnete po dočasném selhání primárního uzlu, viz "Přepnutí na uzel obnovy" na stránce 596.

Návrat na snímek
Pokud v průběhu synchronizace dojde k selhání v primárním uzlu, můžete se vrátit ke snímku pořízenému ze sekundárních dat správce front těsně před spuštěním synchronizace. Sekundární server je poté obnoven do konzistentního stavu a lze jej spustit jako primární. Chcete-li se vrátit ke snímku, vytvořte sekundární snímek do primárního, jak je popsáno v tématu "Přepnutí na uzel obnovy" na stránce 596. Před spuštěním správce front je třeba zkontrolovat, zda bylo vráceno zpět ke snímku (pomocí příkazu **rdqmstatus**).

Linux *Přepnutí na uzel obnovy*

Pokud dojde k havárii na vašem hlavním serveru, proveďte kroky k přepnutí na váš server obnovy.

Informace o této úloze

Po ztrátě primárního správce front na hlavním serveru se sekundární správce front na serveru pro zotavení stane primárním a spustí se. Aplikace se znovu připojí ke správci front na serveru pro zotavení a správce front zpracuje zprávy aplikací. Tento postup můžete také použít k testování uzlu obnovy.

Důležité: Před povýšením původní sekundární instance je třeba se ujistit, že primární instance správce front buď nemůže být spuštěna, nebo je zastavena a vytvořena v sekundární instanci. Jinak mohou narůstat data rozdělená na oblasti.

Musíte být přihlášeni jako uživatel root nebo jako uživatel, který patří do skupiny `mqm` a má nezbytnou konfiguraci sudo.

Postup

1. Používáte-li tento postup k testování sekundárního správce front (tj. primární instance je stále spuštěna), musíte primární instanci zastavit a znovu ji označit jako sekundární instanci:

   ```
   endmqm qmname
   rdqmdr -m qmname -s
   ```

2. Učiňte sekundárního správce front primárním zadáním následujícího příkazu v uzlu zotavení:

   ```
   rdqmdr -m qmname -p
   ```

3. Spusťte správce front zadáním následujícího příkazu:

   ```
   strmqm qmname
   ```

4. Ověřte, že se aplikace znovu připojují ke správci front ve správci front pro zotavení. Pokud jste definovali kanály se seznamem alternativních názvů připojení a zadali jste primární a sekundární správce front, budou se vaše aplikace automaticky připojovat k novému primárnímu správci front.

Jak pokračovat dále

Po obnovení uzlu, který se nezdařil, za předpokladu, že propojení mezi těmito dvěma uzly funguje, nelze správce front v tomto uzlu spustit, protože je spuštěn v uzlu zotavení, v němž jste povýšili sekundární

instanci správce front. Chcete-li se vrátit k normálnímu provozu, musíte zastavit správce front v uzlu zotavení a poté povýšit správce front v původním uzlu zpět na primární roli.

Související odkazy

strmqm

rdqmdr

Testování správce front RDQM pro zotavení

Můžete otestovat, zda instance zotavení správce front v konfiguraci zotavení z havárie RDQM funguje správně bez narušení hlavního serveru.

Informace o této úloze

Správce front pro zotavení testujete zakázáním rozhraní mezi hlavním uzlem a uzlem pro zotavení. Sekundárního správce front převedete do primárního správce front a poté můžete samostatného správce front otestovat. Po dokončení testování obnovíte rozhraní a odstraníte správce front testu. Poté znovu vytvořte správce front jako sekundárního správce front v konfiguraci zotavení z havárie.

Postup

1. Zakažte síťové připojení mezi hlavním uzlem a uzlem obnovy.
2. V uzlu zotavení učiňte správce front primárním:

   ```
   rdqmdr -m QMname -p
   ```

   Kde *QMname* je název správce front.
3. Spusťte správce front:

   ```
   strmqm QMname
   ```
4. Připojte aplikace ke správci front a otestujte, zda pracují podle očekávání.
5. Ukončete správce front:

   ```
   endmqm QMname
   ```
6. Odstraňte správce front:

   ```
   dltmqm QMname
   ```
7. Obnovte síťové připojení mezi hlavním zařízením a zařízením pro obnovu.
8. Na hlavním uzlu spusťte následující příkaz, abyste načetli příkaz **crtmqm** , který jste použili při prvním nakonfigurování zotavení z havárie.

   ```
   rdqmdr -d -m QMname
   ```
9. Spusťte výsledný příkaz **crtmqm** v uzlu zotavení a znovu vytvořte sekundárního správce front. Primární správce front v hlavním uzlu synchronizuje svá data se sekundárním správcem front a aktualizuje je.

Linux *Nahrazení uzlu, který selhal, v konfiguraci zotavení z havárie*

Pokud ztratíte jeden z uzlů v konfiguraci zotavení z havárie, můžete nahradit uzel a obnovit konfiguraci zotavení z havárie podle tohoto postupu.

Informace o této úloze

Dojde-li k takové havárii, že je uzel na hlavním serveru neopravený, můžete nahradit uzel, který selhal, zatímco je správce front spuštěn na uzlu zotavení, a poté obnovit původní konfiguraci zotavení z havárie. Náhradní uzel musí předpokládat identitu selhaného uzlu: název a adresa IP musí být stejné.

Musíte být přihlášeni jako uživatel root nebo jako uživatel, který patří do skupiny `mqm` a má nezbytnou konfiguraci sudo.

Postup

Po ztrátě správce front na hlavním serveru postupujte takto:

1. V uzlu zotavení spusťte následující příkazy, aby sekundární správce front převzal primární roli:

   ```
   rdqmdr -m QMname -p
   ```

   Kde *QMname* je název správce front.
2. Načtěte příkaz, který budete muset spustit na náhradním primárním uzlu, abyste překonfigurovali zotavení z havárie:

   ```
   rdqmdr -m QMname -d
   ```

   Zkopírujte výstup tohoto příkazu.
3. Spuštěním následujícího příkazu spusťte správce front:

   ```
   strmqm QMname
   ```
4. Ověřte, zda se aplikace znovu připojují ke správci front v uzlu zotavení. Pokud jste definovali kanály se seznamem alternativních názvů připojení a zadali jste primární a sekundární správce front, budou se vaše aplikace automaticky připojovat k novému primárnímu správci front.
5. Nahraďte uzel, u kterého došlo k selhání, na hlavním serveru a nakonfigurujte jej tak, aby měl stejný název a adresu IP, který jste použili pro zotavení z havárie na původním uzlu. Poté nakonfigurujte zotavení z havárie spuštěním příkazu **crtmqm** , který jste zkopírovali v kroku 2. Nyní máte sekundární instanci správce front a primární instance synchronizuje její data se sekundární instancí.
6. Ukončete aktuální primární instanci.
7. Po dokončení synchronizace proveďte znovu primární instanci, která je spuštěna na uzlu zotavení, do sekundárního serveru:

   ```
   rdqmdr -m QMname -s
   ```
8. Na náhradním primárním uzlu proveďte sekundární instanci správce front do primární instance:

   ```
   rdqmdr -m QMname -p
   ```
9. Na náhradním primárním uzlu spusťte správce front:

   ```
   strmqm QMname
   ```

   Nyní jste obnovili konfiguraci tak, jak byla před selháním na vašem hlavním serveru.

Související odkazy

strmqm

rdqmdr

endmqm

Řešení nekonzistentního problému v RDQM DR

Stav DR `inconsistent` lze nahlásit, pokud synchronizace mezi primární a sekundární instancí správce front selže.

Informace o této úloze

V sekundární instanci správce front je ohlášen nekonzistentní stav, protože během operace synchronizace došlo ke ztrátě připojení replikace k primární instanci. Možná budete muset provést akci, abyste vyřešili tuto situaci. Zvažte následující posloupnost událostí:

1. Primární správce front DR je synchronizován se sekundárním správcem front DR
2. Odkaz replikace ztracen mezi primárním a sekundárním
3. Propojení replikace obnoveno mezi primárním a sekundárním
4. K resynchronizaci dochází v případě, že sekundární správce front DR zachycuje primárního správce front DR. Během této doby je pro oba správce front nahlášen stav DR `synchronization in progress` .
5. Pokud se replikace během resynchronizace znovu ztratí, stav na sekundárním serveru DR se ohlásí jako `Inconsistent`.

Pokud je uzel, který je hostitelem primárního správce front, stále funkční a odkaz na replikaci lze obnovit, dojde k automatické resynchronizaci. Nekonzistentní stav je vyřešen bez provedení jakékoli akce.

Pokud uzel, který je hostitelem primárního správce front, již není funkční, můžete nekonzistentní stav vyřešit implementací návratu ke snímku v sekundárním správci front. Tato operace vrátí data zpět do posledního známého dobrého stavu.

Postup

Chcete-li vyřešit nekonzistentní stav, postupujte takto:

1. Na uzlu obnovy vytvořte sekundární instanci do primární instance:

   ```
   rdqmdr -m qmname -p
   ```

   Spustí se návrat k operaci snímku.
2. V uzlu zotavení zkontrolujte stav správce front, abyste viděli, kdy je operace vrácení na snímek dokončena:

   ```
   rdqmstatus -m qmname
   ```
3. Je-li stav správce front `Normal`, spusťte správce front:

   ```
   strmqm qmname
   ```

Řešení problému rozděleného na oblasti (rozdělený mozek) v RDQM DR
K problému s rozdělenými oblastmi může dojít, pokud jsou oba správci front ve dvojici pro zotavení z havárie současně spuštění v primární roli.

Informace o této úloze

Pokud jste povýšili sekundární instanci správce front v uzlu zotavení, zatímco původní primární instance pokračovala ve spuštění v hlavním uzlu, jsou spuštěny dvě verze stejného správce front, z nichž každá má vlastní pohled na data správce front. Stav DR pro správce front na každém uzlu je ohlášen jako `Partitioned`.

Musíte se rozhodnout, který z těchto dvou správců front má nejsprávnější pohled na data, a zachovat tuto sadu při vyřazení druhého. K dokončení této operace použijte příkaz **`rdqmdr`** .

Existují dva postupy. První popisuje uchování dat z hlavního uzlu, druhý popisuje uchování dat z uzlu obnovy.

Procedura

- Chcete-li uchovat data ze správce front v hlavním uzlu, postupujte takto:

a) Ujistěte se, že jsou zastaveny obě instance správce front.

b) Určete, že správce front v uzlu zotavení je sekundární:

```
rdqmdr -m qmname -s
```

c) Určete, že správce front v hlavním uzlu je primární:

```
rdqmdr -m qmname -p
```

Synchronizace začíná s daty ze správce front v hlavním uzlu, který se kopíruje do uzlu obnovy.

d) Zkontrolujte stav synchronizace:

```
rdqmstatus -m qmname
```

e) Po dokončení synchronizace spusťte správce front v hlavním uzlu:

```
strmqm qmname
```

- Chcete-li uchovat data ze správce front v uzlu zotavení, postupujte takto:

a) Ujistěte se, že jsou zastaveny obě instance správce front.

b) Určete, že správce front v hlavním uzlu je sekundární:

```
rdqmdr -m qmname -s
```

c) Určete, že správce front v uzlu zotavení je primární:

```
rdqmdr -m qmname -p
```

Synchronizace začíná s daty ze správce front v uzlu zotavení, který se kopíruje do hlavního uzlu.

d) Zkontrolujte stav synchronizace:

```
rdqmstatus -m qmname
```

e) Po dokončení synchronizace vyřaďte správce front v uzlu zotavení:

```
rdqmdr -m qmname -s
```

f) Povyšte správce front v hlavním uzlu a spusťte jej:

```
rdqmdr -m qmname -p
strmqm qmname
```

Změna adres IP v konfiguracích zotavení z havárie
Změníte-li adresy IP některého z rozhraní v konfiguraci zotavení z havárie, replikace mezi těmito dvěma uzly již nebude možná.

Potřebujete-li změnit adresy IP pro replikační rozhraní pro některý z uzlů DR, musíte použít následující postup:

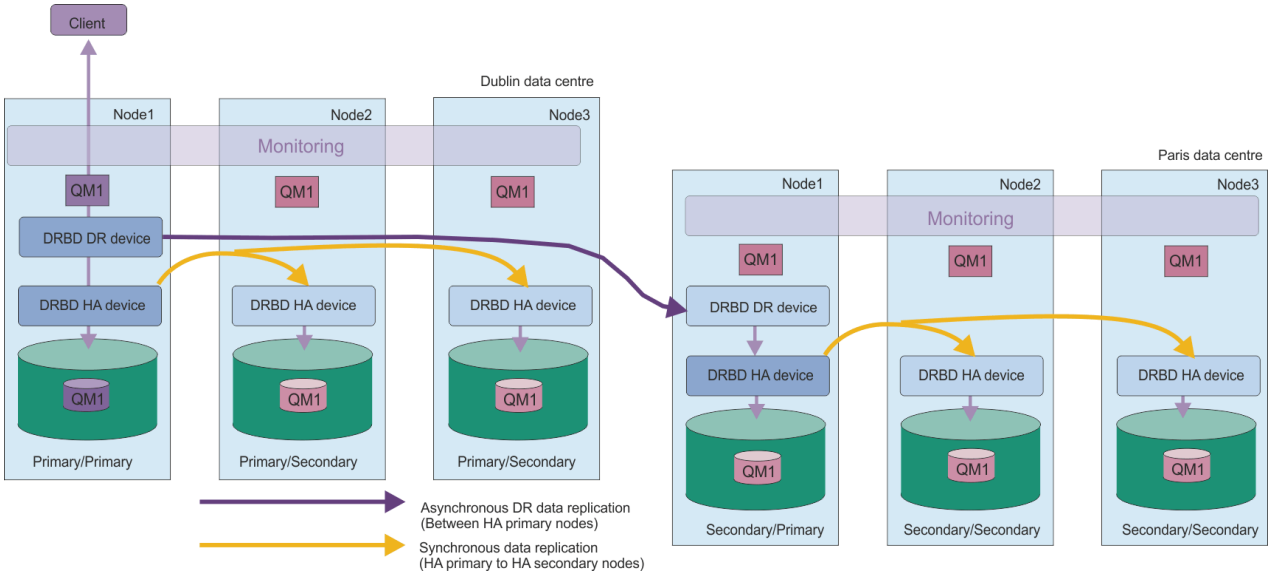
1. V primárním uzlu zazálohujte správce front DR a poté je odstraňte. V uzlu zotavení odstraňte správce front. Další informace jsou uvedeny v tématech “Zálohování a obnova dat správce front IBM MQ” na stránce 650 a “Odstranění RDQM DR” na stránce 584.
2. Znovu vytvořte správce front DR, zadejte nové adresy IP a obnovte zálohy, viz “Vytvoření RDQM pro zotavení z havárie” na stránce 581 a “Zálohování a obnova dat správce front IBM MQ” na stránce 650.

Linux Zotavení z havárie RDQM a vysoká dostupnost

Můžete konfigurovat správce front replikovaných dat (RDQM), který je spuštěn ve skupině s vysokou dostupností na jednom serveru, ale může selhat v jiné skupině s vysokou dostupností na jiném serveru, pokud dojde k nějaké havárii, která způsobí nedostupnost první skupiny. Toto je známé jako DR/HA RDQM.

DR/HA RDQM kombinuje funkce RDQM s vysokou dostupností (viz “Vysoká dostupnost RDQM” na stránce 549) a RDQM pro zotavení z havárie (viz “Zotavení z havárie RDQM” na stránce 577).

Následující diagram zobrazuje příklad DR/HA RDQM.



Replikace mezi DR/HA RDQM na hlavním serveru a serverem pro zotavení z havárie je vždy asynchronní. Při asynchronní replikaci jsou operace, jako např. IBM MQ PUT nebo GET, dokončeny a vráceny do aplikace před replikací události do sekundárního správce front.

Můžete mít dva aktivní servery, spíše než 'hlavní' a 'obnovy', pokud je to nutné, takže některé z vašich DR/HA RDQM běží na jednom serveru a některé na druhém během normálního provozu. Pokud dojde k havárii a jedna organizační jednotka se stane nedostupnou, pak všechny RDQM DR/HA se spustí na stejné skupině HA na stejné organizační jednotce.

Každá skupina HA je nakonfigurována stejným způsobem jako běžná skupina HA. Můžete definovat plovoucí adresy IP pro DR/HA RDQM v každé skupině HA. Plovoucí adresa IP může být stejná nebo odlišná pro každou skupinu HA.

Existující RDQM nelze upgradovat na DR/HA RDQM, musíte vytvořit DR/HA RDQM. (V případě potřeby můžete zálohovat data existujícího RDQM, odstranit je, znovu je vytvořit jako DR/HA RDQM a poté obnovit data, viz “Zálohování a obnova dat správce front IBM MQ” na stránce 650.)

Chcete-li konfigurovat RDQM DR/HA, musíte provést následující hlavní kroky:

1. Nakonfigurujte skupinu HA na 'hlavním' serveru.
2. Nakonfigurujte skupinu HA na serveru 'recovery'.
3. Vytvořte primární/primární DR/HA RDQM na jednom uzlu skupiny HA na 'hlavním' serveru.
4. Vytvořte primární/sekundární DR/HA RDQM na ostatních dvou uzlech na 'hlavním' serveru.
5. Definujte plovoucí adresu IP pro aplikaci pro přístup k DR/HA RDQM, když je spuštěna na libovolném uzlu skupiny HA na 'hlavním' serveru.
6. Vytvořte sekundární/primární DR/HA RDQM na jednom uzlu skupiny HA na serveru 'recovery'.
7. Vytvořte sekundární DR/HA RDQM na dalších dvou uzlech na serveru 'recovery'.
8. Definujte plovoucí adresu IP pro aplikaci pro přístup k DR/HA RDQM, když je spuštěna na libovolném uzlu skupiny HA na serveru 'recovery'.

Podrobnosti o každém z těchto kroků jsou uvedeny v následujících tématech.

Linux *Požadavky na řešení DR/HA RDQM*

Požadavky na řešení DR/HA RDQM jsou stejné jako pro řešení HA RDQM a řešení DR RDQM.

Podrobnosti o požadavcích na části konfigurace vysoké dostupnosti viz “Požadavky na řešení RDQM HA” na stránce 551.

Podrobnosti o části DR konfigurace viz “Požadavky na řešení RDQM DR” na stránce 580.

Linux *Konfigurace skupin HA pro DR/HA RDQM*

Musíte vytvořit skupinu HA na hlavním serveru i na serveru obnovy. Máte-li existující skupinu HA na libovolné org. jednotce, můžete v této skupině HA vytvořit DR/HA RDQM. (Existující RDQM budou nadále fungovat jako dříve.)

Postup je stejný jako postup popsaný pro vysokou dostupnost RDQM, viz “Definování klastru Pacemaker (skupina HA)” na stránce 554.

Při definování skupiny s vysokou dostupností zadáváte adresy IP používané pro monitorování a replikaci jednotlivými uzly v souboru `rdqm.ini` . Při vytváření skupiny HA pro podporu DR/HA RDQM můžete také uvést adresy IP použité pro replikaci DR skupinou HA, kterou definujete, a adresy IP použité pro replikaci DR uzly v jiné skupině HA dvojice DR. (Pokud neuvedete adresy IP replikace DR v souboru `rdqm.ini` , můžete je uvést v příkazovém řádku při vytváření DR/HA RDQM.)

Pokud konfigurujete existující skupinu HA, můžete přidat adresy IP replikace DR do existujícího souboru `rdqm.ini` . Po aktualizaci produktu `rdqm.ini`nemusíte znovu spustit příkaz **`rdqmadm`** , ale musíte aktualizovat produkt `rdqm.ini` , než vytvoříte jakékoli RDQM DR/HA.

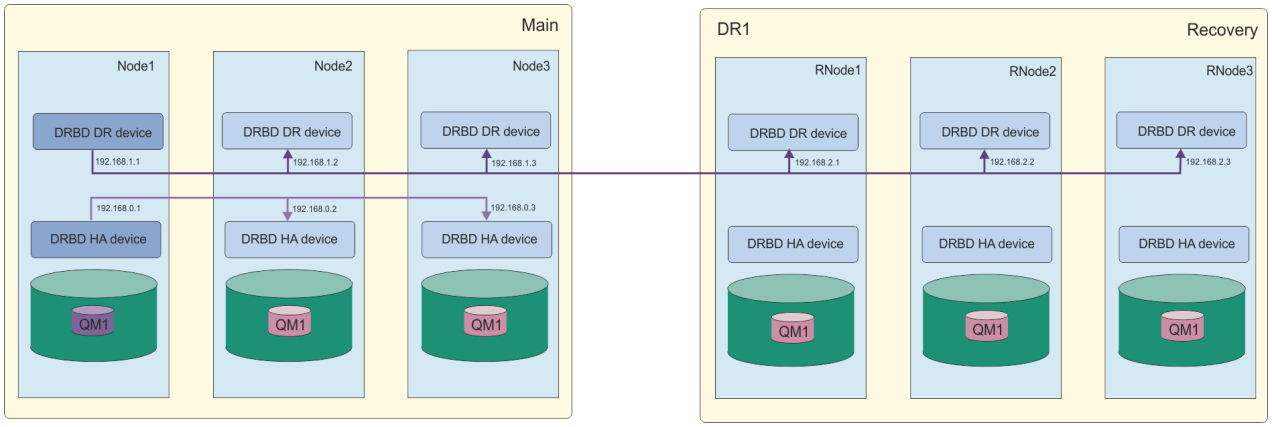
Použijte atribut `DR_Replication` v sekcích `Node` k uvedení rozhraní replikace DR ve skupině HA, kterou definujete, například:

```
Node:
  Name=Node1
  HA_Replication=192.168.0.1
  DR_Replication=192.168.1.1
Node:
  Name=Node2
  HA_Replication=192.168.0.2
  DR_Replication=192.168.1.2
Node:
  Name=Node3
  HA_Replication=192.168.0.3
  DR_Replication=192.168.1.3
```

Sekci `DRGroup` použijte k uvedení adres replikace DR vzdálené skupiny HA, například:

```
DRGroup:
  Name=DR1
  DR_Replication=192.168.2.1
  DR_Replication=192.168.2.2
  DR_Replication=192.168.2.3
```

Tuto konfiguraci ilustruje následující diagram:



Pokud neuvedete adresy IP replikace DR pro uzly v lokální skupině HA buď v souboru `rdqm.ini` , nebo na příkazovém řádku, když vytváříte DR/HA RDQM, pak se rozhraní `HA_Replication` definovaná pro

každý uzel použijí pro replikaci DR. Adresy vzdálené replikace DR skupiny HA musíte uvést buď v souboru `rdqm.ini` , nebo na příkazovém řádku **crtmqm** .

Linux *Vytváření DR/HA RDQMs*

Příkaz **crtmqm** se používá k vytvoření správce front replikovaných dat (RDQM) v konfiguraci DR/HA.

Informace o této úloze

Můžete vytvořit DR/HA RDQM jako uživatele ve skupině `mqm` , pokud může uživatel použít příkaz sudo. Jinak musíte vytvořit RDQM jako kořen.

Musíte vytvořit počet RDQM DR/HA:

- Ve skupině HA na "hlavní" stránce:
  - V uzlu, v němž chcete, aby byl správce front spuštěn za normálních podmínek, vytvořte primární/primární DR/HA RDQM.
  - Na každém ze dvou dalších uzlů ve skupině HA vytvořte primární/sekundární DR/HA RDQM.
- Ve skupině HA na serveru "obnova":
  - V uzlu, v němž bude spuštěn správce front v případě, že dojde k selhání na serveru zotavení, vytvořte sekundární/primární DR/HA RDQM. Výstup příkazu můžete použít, když jste vytvořili primárního/primárního správce front na 'hlavním' serveru.
  - Na každém ze dvou dalších uzlů ve skupině HA vytvořte sekundární/sekundární DR/HA RDQM.

Všechny instance správce front musí mít stejný název a musí jim být přiděleno stejné množství úložiště.

Následující body poskytují určité vodítko při určování velikosti systému souborů správce front:

1. Při vytváření správce front RDQM je systém souborů přidělen k ukládání dat a protokolů správce front. Je důležité tento systém souborů vhodně nastavit tak, aby mohl správce front zaznamenávat probíhající aktivity do protokolů a ukládat zprávy aplikací do front. Při určování velikosti systému souborů zvažte požadavky na špičkový systém zpráv, budoucí růst pracovní zátěže a výpadky aplikací, které by mohly způsobit sestavení zpráv ve frontách. Informace o výpočtu velikosti protokolu pro zotavení správce front naleznete v části “Jak velký by měl být souborový systém protokolu?” na stránce 632. Při výpočtu požadavků na úložiště pro zprávy aplikace je třeba vzít v úvahu velikost a počet zpráv plus jejich záhlaví MQMD a všechny vlastnosti zpráv, které mají.
2. Velikost systémů souborů správce front RDQM nelze dynamicky měnit. Je-li to vyžadováno, je třeba provést zálohu a poté obnovit správce front RDQM s větším systémem souborů, viz “Změna velikosti systému souborů pro správce front HA RDQM” na stránce 563.
3. Velikost jednotlivých front na disku můžete omezit pomocí atributů lokální fronty, například MAXDEPTH a MAXFSIZE. Viz Úprava IBM MQ.
4. Měli byste monitorovat probíhající využití disku a odpovídajícím způsobem reagovat, pokud se využití disku zvýší dříve, než se využití systému souborů stane kritickým. Využití systému souborů lze monitorovat buď pomocí schopností platformy/operačního systému, nebo přihlášením k odběru metrik publikovaných v tématech systému IBM MQ , která jsou popsána v tématu Metriky publikované v tématech systému.

Procedura

- Chcete-li vytvořit primární/primární DR/HA RDQM:

  a) Zadejte následující příkaz:

```
crtmqm -sx -rr p
             [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
             (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
             -rp DRPort
             [-z] [-q] [-c Text] [-d DefXmitQ] [-h MaxHandles]
             [-g ApplicationGroup] [-oa user|group]
             [-t TrigInt] [-u DeadQ] [-x MaxUMsgs]
             [-lp LogPri] [-ls LogSec]
```

```
              [-lc | -ll | -lla | -lln] [-lf LogFileSize]
              [-p Port] [-fs FilesystemSize] QMgrName
```

Kde:

-sx
Označuje, že počáteční role HA je primární.

-rr p
Označuje, že počáteční role DR je primární.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Volitelně zadejte adresy IP rozhraní DR na třech uzlech na lokálním serveru (tj. na 'hlavním' serveru). Není-li uvedeno, použijí se adresy IP uvedené v souboru `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Zadejte adresy IP rozhraní DR na třech uzlech na vzdáleném serveru (tj. na serveru 'recovery'). Musíte zadat buď tento parametr, nebo parametr `-rn` .

-rn *GroupName*
Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

-rp *Port*
Určuje port, který má být použit pro replikaci DR.

další_volení_crtmqm_volby
Volitelně můžete uvést jednu nebo více z těchto obecných voleb **`crtmqm`** :

- -z
- -q
- -c *Text*
- -d *DefaultTransmissionFronta*
- -h *MaxHandles*
- -g *ApplicationGroup*
- -oa uživatel | skupina
- -t *TrigInt*
- -u *DeadQ*
- -x *MaxUMsgs*
- -lp *LogPri*
- -ls *LogSec*
- -lc | -l
- -lla | -lln
- -lf *LogFile*
- -p *Port*

-fs *velikost*
Volitelně určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického disku vytvořeného ve skupině disků drbdpool. Je také vytvořen další logický disk této velikosti, který podporuje opětovné vrácení na operaci snímku, takže celková paměť pro RDQM DR je téměř dvojnásobná, než je zde uvedeno.

Velikost : Číselná hodnota určená v GB. Hodnotu v MB můžete zadat zadáním hodnoty následované znakem `M`. Chcete-li například zadat velikost systému souborů 3 GB, zadejte hodnotu 3. Chcete-li určit velikost systému souborů 1024 MB, zadejte hodnotu 1024M. (K explicitnímu stavu GB můžete také přidat příponu G.)

QMNAME
Určuje název správce front replikovaných dat. V názvu jsou rozlišována velká a malá písmena.

Po dokončení příkazu je výstupem příkazu, který můžete zadat na server pro zotavení a vytvořit tak sekundární/primární instanci správce front.

- Chcete-li vytvořit primární/sekundární DR/HA RDQM na ostatních dvou uzlech ve skupině HA:

  a) Zadejte následující příkaz na každém uzlu:

```
crtmqm -sxs -rr p
             [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
             (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
             -rp DRPort
             [-fs FilesystemSize] QMgrName
```

  Kde:

  -sxs
  Označuje, že počáteční role HA je sekundární.

  -rr p
  Označuje, že počáteční role DR je primární.

  -rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
  Volitelně zadejte adresy IP rozhraní DR na třech uzlech na lokálním serveru (tj. na 'hlavním' serveru). Není-li uvedeno, použijí se adresy IP uvedené v souboru `rdqm.ini` .

  -ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
  Zadejte adresy IP rozhraní DR na třech uzlech na vzdáleném serveru (tj. na serveru 'recovery'). Musíte zadat buď tento parametr, nebo parametr `-rn` .

  -rn *GroupName*
  Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

  -rp *Port*
  Určuje port, který má být použit pro replikaci DR.

  -fs *velikost*
  Určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického disku vytvořeného ve skupině disků drbdpool. Pokud jste při vytváření primárního/primárního RDQM zadali jinou než výchozí velikost, musíte zde zadat stejnou hodnotu.

  Velikost : Číselná hodnota určená v GB. Hodnotu v MB můžete zadat zadáním hodnoty následované znakem `M`. Chcete-li například zadat velikost systému souborů 3 GB, zadejte hodnotu 3. Chcete-li určit velikost systému souborů 1024 MB, zadejte hodnotu 1024M. (K explicitnímu stavu GB můžete také přidat příponu G.)

  QMNAME
  Určuje název primárního/sekundárního RDQM. Musí se shodovat s názvem, který jste zadali pro primární/primární instanci RDQM. Všimněte si, že název rozlišuje malá a velká písmena.

- Chcete-li vytvořit sekundární/primární DR/HA RDQM v uzlu, kde bude spuštěn správce front, pokud se nezdaří na serveru zotavení:

  a) Výstup příkazu použijte, když jste vytvořili primární/primární DR/HA na hlavním serveru, nebo zadejte následující příkaz:

```
crtmqm -sx -rr s
             [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
             (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
             -rp DRPort
             [-fs FilesystemSize] QMgrName
```

  -sx
  Označuje, že počáteční role HA je primární.

  -rr s
  Označuje, že počáteční role DR je sekundární.

  -rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
  Volitelně uveďte adresy IP rozhraní DR na třech uzlech na lokálním serveru (tj. na serveru 'recovery'). Není-li uvedeno, použijí se adresy IP uvedené v souboru `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Zadejte adresy IP rozhraní DR na třech uzlech na vzdáleném serveru (tj. na 'hlavním' serveru). Musíte zadat buď tento parametr, nebo parametr `-rn` .

-rn *GroupName*
Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

-rp *Port*
Určuje port, který má být použit pro replikaci DR.

-fs *velikost*
Volitelně určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického disku vytvořeného ve skupině disků drbdpool. Je také vytvořen další logický disk této velikosti, který podporuje opětovné vrácení na operaci snímku, takže celková paměť pro RDQM DR je téměř dvojnásobná, než je zde uvedeno.

QMNAME
Určuje název správce front replikovaných dat. V názvu jsou rozlišována velká a malá písmena.

- Chcete-li vytvořit sekundární HA/DR RDQM na dalších dvou uzlech na serveru obnovy, postupujte takto:

  a) Zadejte následující příkaz na každém uzlu:

```
crtmqm -sxs -rr s
             [-rl DRLocalIP1,DRLocalIP2,DRLocalIP3]
             (-ri DRRemoteIP1,DRRemoteIP2,DRRemoteIP3 | -rn GroupName)
             -rp DRPort
             [-fs FilesystemSize] QMgrName
```

-sxs
Označuje, že počáteční role HA je primární.

-rr s
Označuje, že počáteční role DR je sekundární.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Volitelně uveďte adresy IP rozhraní DR na třech uzlech na lokálním serveru. Není-li uvedeno, použijí se adresy IP uvedené v souboru `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Zadejte adresy IP rozhraní DR na třech uzlech na vzdáleném serveru. Musíte zadat buď tento parametr, nebo parametr `-rn` .

-rn *GroupName*
Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

-rp *Port*
Určuje port, který má být použit pro replikaci DR.

-fs *velikost*
Volitelně určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického disku vytvořeného ve skupině disků drbdpool. Je také vytvořen další logický disk této velikosti, který podporuje opětovné vrácení na operaci snímku, takže celková paměť pro RDQM DR je téměř dvojnásobná, než je zde uvedeno.

QMNAME
Určuje název správce front replikovaných dat. V názvu jsou rozlišována velká a malá písmena.

Poznámka: Když vytvoříte RDQM, další volné číslo portu nad 7000 je přiděleno pro odkaz na replikaci HA. Pokud se zjistí, že zvolený port používá jiná aplikace, příkaz **`crtmqm`** selže s chybou AMQ6543 a tento port se přidá do seznamu vyloučení. Musíte odstranit sekundární instance správce front a poté znovu spustit příkaz **`crtmqm`** .

Jak pokračovat dále

Po vytvoření všech RDQM DR/HA musíte zkontrolovat stav primární/primární a sekundární/primární instance, abyste zkontrolovali, zda jsou všechny správné. Použijte příkaz **rdqmstatus** na uzlech. Uzly by měly zobrazovat normální stav, jak je popsáno v tématu “Zobrazení stavu DR/HA RDQM a skupiny HA” na stránce 609. Pokud tento stav nezobrazují, odstraňte sekundární/primární instanci a znovu ji vytvořte. Je třeba dbát na použití správných argumentů.

Související úlohy

“Vytváření DR/HA RDQMs” na stránce 603

Příkaz **crtmqm** se používá k vytvoření správce front replikovaných dat (RDQM) v konfiguraci DR/HA.

Související odkazy

crtmqm

Linux *Odstranění DR/HA RDQM*

Příkaz **dltmqm** se používá k odstranění správce front replikovaných dat DR/HA (RDQM).

Informace o této úloze

Musíte spustit příkaz pro odstranění RDQM na primárním/primárním uzlu i na sekundárním/primárním uzlu. Nejprve musí být ukončen RDQM. Příkaz můžete spustit jako uživatel mqm, pokud má tento uživatel nezbytná oprávnění k příkazu sudo. Jinak musíte příkaz spustit jako uživatel root.

Procedura

- Chcete-li odstranit DR/HA RDQM, zadejte následující příkaz:

```
dltmqm RDQM_name
```

Související odkazy

dltmqm

Linux ***Vytvoření plovoucí adresy IP***

Plovoucí adresy IP můžete vytvořit pro každou skupinu HA v konfiguraci DR/HA RDQM.

Plovoucí adresa IP umožňuje klientovi používat stejnou adresu IP pro DR/HA RDQM bez ohledu na to, na kterém uzlu ve skupině HA je spuštěn. Pokud mají vaše dvě skupiny HA soukromé/izolované sítě pro konektivitu aplikace, pak lze pro obě skupiny definovat stejnou plovoucí adresu IP. Stále musíte definovat tuto plovoucí adresu IP dvakrát, avšak jednou na každé z vašich skupin HA.

Plovoucí adresy IP vytváříte a odstraňujete pomocí stejné metody jako pro RDQM s vysokou dostupností. Viz “Vytvoření a odstranění plovoucí adresy IP” na stránce 566.

Linux ***Spuštění, zastavení a zobrazení stavu DR/HA RDQM***

Varianty standardních řídicích příkazů IBM MQ se používají ke spuštění, zastavení a zobrazení aktuálního stavu DR/HA RDQM.

Informace o této úloze

Musíte spustit příkazy, které spustí, zastaví a zobrazí aktuální stav DR/HA RDQM jako uživatel, který patří do skupin `mqm` i `haclient` .

Musíte spustit příkazy pro spuštění a zastavení správce front v primárním uzlu pro tohoto správce front.

Procedura

- Chcete-li spustit RDQM, zadejte na primárním uzlu RDQM následující příkaz:

```
strmqm qmname
```

kde *qmname* je název DR/HA RDQM, který chcete spustit.

Je spuštěn RDQM a Pacemaker spustí správu RDQM. Chcete-li zadat další volby `strmqm` , musíte zadat volbu `-ns` spolu s volbou `strmqm` .

- Chcete-li zastavit RDQM, zadejte na primárním uzlu DR/HA RDQM následující příkaz:

```
endmqm qmname
```

kde *qmname* je název RDQM, který chcete zastavit.

Modul Pacemaker ukončí správu RDQM a poté je RDQM ukončen. Všechny ostatní parametry **endmqm** lze použít při zastavování RDQM.

- Chcete-li zobrazit stav RDQM, zadejte následující příkaz:

```
dspmq -m QMname
```

Výstupní informace o stavu závisí na tom, zda jste spustili příkaz na primárním nebo sekundárním uzlu RDQM. Pokud se spustí na primárním uzlu, zobrazí se jedna z běžných stavových zpráv vrácených produktem **dspmq** . Spustíte-li příkaz na sekundárním uzlu, zobrazí se stav `Ended immediately` . Pokud je například produkt **dspmq** spuštěn na uzlu RDQM7, mohou být vráceny následující informace:

```
QMNAME(DRQM8)                           STATUS(Ended immediately)
QMNAME(DRQM7)                           STATUS(Running)
```

Pomocí argumentů s produktem `dspmq` můžete určit, zda je RDQM konfigurován pro zotavení z havárie a zda je momentálně primární nebo sekundární instancí:

```
dspmq -m QMname -o (dr | DR)
```

Zobrazí se jedna z následujících odpovědí:

DRROLE()
Označuje, že správce front není konfigurován pro zotavení z havárie.

DRROLE(Primary)
Označuje, že je správce front konfigurován jako primární DR.

DRROLE(Secondary)
Označuje, že správce front je konfigurován jako sekundární DR.

Použijte příkaz **dspmq -o all** k zobrazení informací o zotavení z havárie a vysoké dostupnosti pro DR/HA RDQMs. Pokud například spustíte produkt **dspmq -o all** na uzlu, kde je spuštěn produkt DR/HA RDQM, uvidíte následující informace o stavu:

```
QMNAME(TESTQM1)                                           STATUS(Running) HA(Replicated)
DRROLE(Primary)
```

Související odkazy

dspmq (zobrazení správců front)
endmqm (koncový správce front)
strmqm (spustit správce front)

V 9.3.0 *Nezdařené akce prostředků v konfiguracích DR/HA*

Akce nezdařených prostředků se vyskytnou, když komponenta Pacemaker konfigurace vysoké dostupnosti RDQM zjistí nějaký problém s prostředkem na jednom z uzlů ve skupině HA.

Akce nezdařených prostředků mohou vzniknout na jedné z konfigurací vysoké dostupnosti v konfiguraci RDQM DR/HA. Můžete použít příkaz **rdqmstatus** k zobrazení akcí nezdařených prostředků a příkaz **rdqmclean** k jejich vymazání (po vyřešení příčiny selhání). Proces je stejný jako pro konfigurace vysoké dostupnosti RDQM bez komponenty DR. Další podrobnosti naleznete v části “Nezdařené akce prostředků” na stránce 569.

Související úlohy

“Zobrazení stavu DR/HA RDQM a skupiny HA” na stránce 609
Můžete zobrazit stav HA a roli DR správců front replikovaných dat DR/HA (RDQM).

“Zobrazení stavu skupiny RDQM a HA” na stránce 570
Můžete zobrazit stav skupiny HA a jednotlivých správců front replikovaných dat (RDQM).

Související odkazy

rdqmclean

rdqmstatus

Linux *Zobrazení stavu DR/HA RDQM a skupiny HA*

Můžete zobrazit stav HA a roli DR správců front replikovaných dat DR/HA (RDQM).

Informace o této úloze

Příkaz **rdqmstatus** použijte k zobrazení stavu jednotlivých RDQMs nebo k získání přehledu o stavu všech RDQMs známých skupině HA.

V 9.3.0 Souhrnný stav uzlu také zobrazuje informace o modulu jádra DRBD, na kterém RDQM spoléhá. Při upgradu RDQM je důležité zajistit, aby byla pro verzi jádra RHEL spuštěného v systému nainstalována správná verze modulu jádra DRBD. Stav zobrazuje verzi jádra operačního systému, verzi jádra, pro kterou byl modul DRBD sestaven, verzi DRBD a stav načtení modulu jádra DRBD.

Poznámka: Všimněte si, že v konfiguraci HA/DR konfigurace DR vždy používá asynchronní replikaci, zatímco konfigurace HA vždy používá synchronní replikaci. Tyto hodnoty nejsou zobrazeny ve výstupu příkazu `rdqmstatus -m qmgr` v kombinované konfiguraci HA/DR.

Chcete-li spustit příkaz **rdqmstatus** , musíte být uživatelem ve skupinách `mqm` a `haclient` . Příkaz můžete spustit na libovolném uzlu v jedné ze skupin HA.

Procedura

- Chcete-li zobrazit souhrnný stav uzlu a RDQM, které jsou součástí konfigurace vysoké dostupnosti, postupujte takto:

  ```
  rdqmstatus
  ```

  Zobrazí se identita uzlu, na kterém jste spustili příkaz, a stav RDQMs v konfiguraci vysoké dostupnosti plus jejich aktuální role DR, například:

  ```
  Node:                                 main-alice
  OS kernel version:                    3.10.0-1160.15.2
  DRBD OS kernel version:               3.10.0-1160
  DRBD version:                         9.1.1
  DRBD kernel module status:            Loaded

  Queue manager name:                   RDQM1
  Queue manager status:                 Running elsewhere
  HA current location:                  main-charlie
  HA preferred location:                main-charlie
  HA blocked location:                  None

  Queue manager name:                   RDQM9
  Queue manager status:                 Running elsewhere
  HA current location:                  main-bob
  HA preferred location:                main-bob
  HA blocked location:                  None
  DR role:                              Primary

  Queue manager name:                   RDQM7
  Queue manager status:                 Running
  HA current location:                  This node
  HA preferred location:                This node
  HA blocked location:                  None
  DR role:                              Primary
  ```

V tomto příkladu jsou RDQM7 a RDQM8 DR/HA RDQMs, zatímco RDQM1 je HA RDQM, který není konfigurován pro přepnutí na server pro zotavení z havárie.

V 9.3.0 Stav modulu jádra DRBD je jedna z následujících hodnot:

Načteno
Označuje, že byl načten modul DRBD.

Částečně načteno
Může se vyskytnout, když byl modul DRBD načten, ale nefunguje správně kvůli neshodě.

Nenačteno
Modul DRBD není načten. Tuto možnost lze zobrazit v nově nainstalované konfiguraci v případě, že dosud nebyli vytvořeni žádní správci front RDQM.

Neinstalováno
Označuje, že buď modul DRBD není nainstalován. nebo že produkt IBM MQ nemohl určit verzi jádra operačního systému modulu DRBD.

Dříve nainstalovaná verze je stále načtena
Tento stav může nastat, pokud je nainstalován nový modul DRBD, zatímco je spuštěn existující modul DRBD (tj. je spuštěn správce front RDQM). Nově nainstalovaný modul je ohlášen ve stavu, ale nejedná se o modul, který je ve skutečnosti spuštěn.

- Chcete-li zobrazit stav konkrétního správce front na všech uzlech ve skupině s vysokou dostupností, zadejte následující příkaz:

```
rdqmstatus -m qmname
```

kde *qmname* je název RDQM, pro který chcete zobrazit stav. Zobrazí se stav RDQM na aktuálním uzlu následovaný souhrnem stavu ostatních dvou uzlů z perspektivy aktuálního uzlu.

- V 9.3.0
Chcete-li zobrazit stav konkrétního správce front na všech uzlech ve skupině s vysokou dostupností, včetně podrobností o všech nezdařených akcích prostředků, zadejte následující příkaz:

```
rdqmstatus -m qmname -a
```

kde *qmname* je název RDQM, pro který chcete zobrazit stav. Zobrazí se stav RDQM na aktuálním uzlu následovaný souhrnem stavu ostatních dvou uzlů z perspektivy aktuálního uzlu. Za tím následují podrobnosti o všech nezdařených akcích prostředků přidružených k RDQM.

Následující tabulka shrnuje informace o aktuálním uzlu, které mohou být vráceny příkazem `rdqmstatus -m qmname` pro RDQM.

Tabulka 35. Aktuální stav uzlu

Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Název uzlu	*NodeName*	Vždy zobrazeno
Stav správce front	stav správce front (jeden ze stavů, které jsou platné pro příkaz **dspmq**)	Vždy zobrazeno
CPU	*n.nn*%	Zobrazí se pouze v případě, že je RDQM spuštěn na tomto uzlu
Paměť	*nnn*MB využito	Zobrazí se pouze v případě, že je RDQM spuštěn na tomto uzlu
Systém souborů správce front	*nnn*použitých MB, *y.y*přidělených GB [*z*%]	Zobrazí se pouze v případě, že je RDQM spuštěn na tomto uzlu

Tabulka 35. Aktuální stav uzlu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Role HA	Primární Sekundární Neznámý	Vždy zobrazeno
Stav HA	Všechny uzly jsou v pohotovostním režimu Tento uzel je v pohotovostním režimu Vzdálené uzly v pohotovostním režimu Smíšená	Všechny uzly jsou v pohotovostním režimu Aktuální uzel v pohotovostním režimu Oba vzdálené uzly v pohotovostním režimu Jiný stav pro každý vzdálený uzel
Řízení HA	Povoleno Zakázáno Neznámý	Vždy zobrazeno. Zobrazuje, zda je RDQM pod ovládacím prvkem Pacemaker
Upřednostňované umístění HA	Není Tento uzel Neznámý *NodeName*	Vždy zobrazeno
V 9.3.0 V 9.3.0 Blokované umístění vysoké dostupnosti	Žádný-Správce front není blokován ke spuštění v žádném uzlu Tento uzel-správci front je zablokováno spuštění v aktuálním uzlu kvůli jedné nebo více nezdařeným akcím prostředků *nodename* -Správce front je blokován před spuštěním na *nodename* kvůli jedné nebo více nezdařeným akcím prostředků. *nodename1*, *nodename2* -Správce front je blokován před spuštěním v systému *nodename1* a *nodename2* kvůli jedné nebo více nezdařeným akcím prostředku. Všechny uzly-správci front je zablokováno spuštění ve všech uzlech kvůli jedné nebo více nezdařeným akcím prostředků.	Vždy zobrazeno
Plovoucí rozhraní IP HA	*název_rozhraní*	Vždy zobrazeno
Plovoucí adresa IP HA	*IPV4_address*	Vždy zobrazeno
Role DR	Primární Sekundární Sekundární nevyřízený Neznámý	Vždy zobrazeno

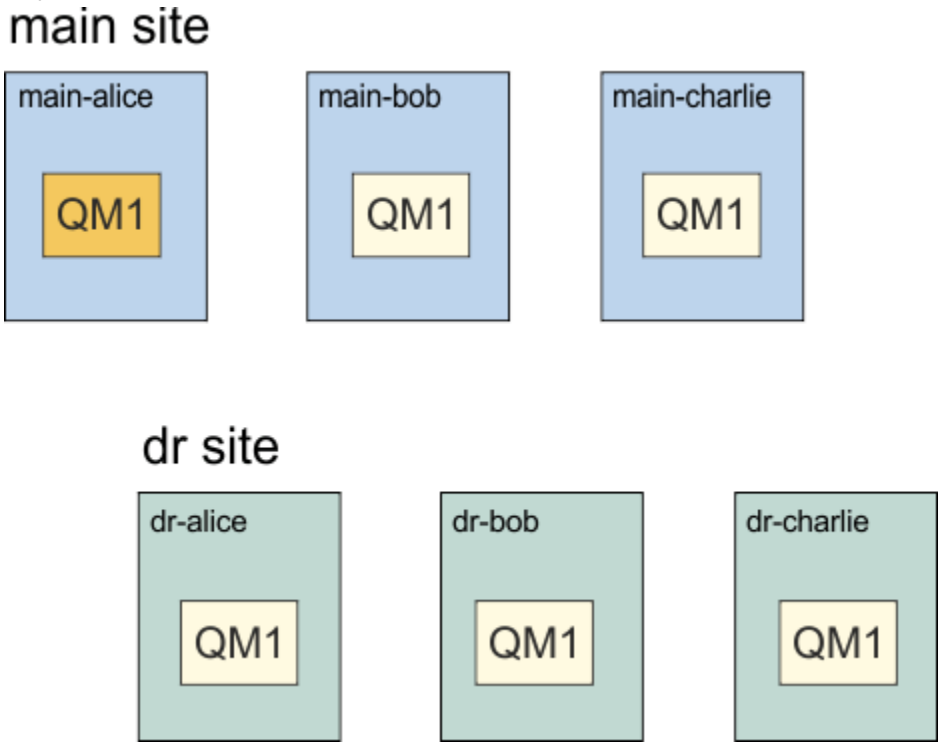
Tabulka 35. Aktuální stav uzlu (pokračování)

Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Stav DR	Normální Probíhá synchronizace Rozděleno na oblasti Vzdálený systém není k dispozici Nekonzistentní Návrat na snímek Vzdálený systém není nakonfigurován Vyjednávání se nezdařilo	Všechno je v pořádku. Probíhá synchronizace. Uživatel spustil frontu správce na každém uzlu, zatímco Síť replikace DR byla není k dispozici. Připojení k jinému uzlu byl ztracen. Synchronizace probíhala, ale byla přerušena. Uživatel se rozhodl vrátit se k snímek, který byl pořízen při správce front zadal Nekonzistentní stav. Primární byl nakonfigurován ale sekundární nemá. Počáteční vyjednávání mezi primárním a sekundárním uzlem se nezdařilo. To může být způsobeno nekompatibilními typy replikace nebo pokud je sekundární uzel konfigurován s menší velikostí systému souborů.
Stav DR (na sekundárním uzlu HA)	Viz *HA_Primary_Node*	Zobrazuje se na sekundárních uzlech HA, protože stav DR je známý pouze na primárním uzlu HA.
Port DR	Port TCP/IP použitý k replikaci dat pro tohoto správce front.	Vždy zobrazeno.
Lokální adresa IP DR	Lokální adresa IP, kterou bude tento správce front používat pro replikaci DR	Vždy zobrazeno.
Seznam vzdálených adres IP DR	Adresy IP vzdáleného systému, které bude tento správce front používat pro replikaci DR. Seznam tří adres IP oddělených čárkami.	Vždy zobrazeno.
Aktuální adresa IP vzdáleného systému DR	Aktuální vzdálená adresa IP, ke které je tento správce front připojen pro replikaci DR.	Pro primární HA s aktivním připojením DR.
Aktuální adresa IP vzdáleného systému DR (na sekundárním uzlu HA)	Viz *HA_Primary_Node*	Zobrazeno na sekundárním uzlu HA, protože připojení DR je pouze na primárním uzlu HA
Nesynchronizovaná data DR	*x*KB	Zobrazí se, když je vzdálený uzel nedostupný nebo nekonzistentní.
Průběh synchronizace DR	*y*%	Zobrazí se, když probíhá synchronizace.
Předpokládaný čas dokončení DR	*dd.MM.yyyy HH:mm:ss*	Zobrazí se, když probíhá synchronizace.

Tabulka 35. Aktuální stav uzlu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Průběh opětovného vrácení snímku	*y%*	Zobrazí se, když je stav DR "Návrat ke snímku"
V 9.3.0 V 9.3.0 DR naposledy synchronizováno	*dd.MM.yyyy HH:mm:ss*	Zobrazí se, když jsou data DR nesynchronizovaná (po počáteční synchronizaci). Udává čas a datum, kdy byla data naposledy synchronizována.

Příklad

Tyto příklady ilustrují příkaz **`rdqmstatus -m qm1`** spuštěný na různých uzlech následující konfigurace DR/HA:



Příklad normálního stavu na uzlu, který je primární DR a primární HA:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.1.1
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           192.168.2.1

Node:                                   main-bob
HA status:                              Normal
```

```
Node:                                   main-charlie
HA status:                              Normal
```

Příklad normálního stavu na uzlu, který je primární DR a sekundární HA:

```
Node:                                   main-bob
Queue manager status:                   Running elsewhere
HA role:                                Secondary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    main-alice
HA preferred location:                  main-alice
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              See main-alice
DR port:                                3000
DR local IP address:                    192.168.1.2
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           See main-alice

Node:                                   main-alice
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

Příklad normálního stavu na uzlu, který je sekundární DR a primární HA:

```
Node:                                   dr-alice
Queue manager status:                   Ended immediately
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Secondary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.2.1
DR remote IP address list:              192.168.1.1,192.168.1.2,192.168.1.3
DR current remote IP address:           192.168.1.1

Node:                                   dr-bob
HA status:                              Normal

Node:                                   dr-charlie
HA status:                              Normal
```

Příklad normálního stavu na uzlu, který je sekundární DR, a sekundární HA:

```
Node:                                   dr-bob
Queue manager status:                   Ended immediately
HA role:                                Secondary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    dr-alice
HA preferred location:                  dr-alice
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Secondary
DR status:                              See dr-alice
DR port:                                3000
DR local IP address:                    192.168.2.2
DR remote IP address list:              192.168.1.1,192.168.1.2,192.168.1.3
DR current remote IP address:           See dr-alice

Node:                                   dr-alice
HA status:                              Normal

Node:                                   dr-charlie
HA status:                              Normal
```

Příklad probíhající synchronizace DR na uzlu, který je primární DR a primární HA:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.1.1
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           192.168.2.1
DR synchronization progress:            11.0%
DR estimated time to completion:        2018-09-06 14:55:05

Node:                                   main-bob
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

Příklad rozdělení DR na oblasti na uzlu, který je primárním uzlem DR a primárním uzlem HA:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Partitioned
DR port:                                3000
DR local IP address:                    192.168.1.1
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           192.168.2.1
DR out of sync data:                    372KB

Node:                                   main-bob
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

V 9.3.0 Příklad nesynchronizované DR na uzlu, který je primární DR a primární HA:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Remote unavailable
DR port:                                3000
DR local IP address:                    192.168.1.1
```

```
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           Unknown
DR out of sync data:                    372KB
DR last in sync:                        2020-02-02 20:22:02

Node:                                   main-bob
HA status:                              Normal

Node:                                   main-charlie
HA status:                              Normal
```

V 9.3.0 Příklad nesynchronizované HA na uzlu, který je primární DR a primární HA:

```
Node:                                   main-alice
Queue manager status:                   Running
CPU:                                    0.00%
Memory:                                 123MB
Queue manager file system:              51MB used, 1.0GB allocated [5%]
HA role:                                Primary
HA status:                              Normal
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
HA floating IP interface:               None
HA floating IP address:                 None
DR role:                                Primary
DR status:                              Normal
DR port:                                3000
DR local IP address:                    192.168.1.1
DR remote IP address list:              192.168.2.1,192.168.2.2,192.168.2.3
DR current remote IP address:           192.168.2.1

Node:                                   main-bob
HA status:                              Inconsistent
HA out of sync data:                    15932KB
HA last in sync:                        2020-02-02 20:22:02

Node:                                   main-charlie
HA status:                              Normal
```

V 9.3.0 Příklad souhrnného stavu, který ukazuje neshodu mezi verzí jádra operačního systému (RHEL 7.9) a modulem jádra DRBD (zaměřeno na RHEL 7.8). I když zpráva o stavu hlásí, že je načten modul jádra DRBD a je spuštěn správce front, měli byste aktualizovat modul jádra DRBD o verzi, která je v této situaci určena pro spuštěné jádro operačního systému.

```
Node:                                   main-alice
OS kernel version:                      3.10.0-1160.15.2
DRBD OS kernel version:                 3.10.0-1127
DRBD version:                           9.1.1
DRBD kernel module status:              Loaded

Queue manager name:                     QM1
Queue manager status:                   Running
HA current location:                    This node
HA preferred location:                  This node
HA blocked location:                    None
DR role:                                Primary
```

V 9.3.0 Příklad souhrnného stavu ukazujícího neshodu mezi verzí jádra operačního systému (RHEL 7.9) a modulem jádra DRBD (zaměřeným na RHEL 7.6). V tomto příkladu je neshoda verzí závažnější a modul jádra DRBD se nepodařilo úspěšně načíst. QM1 je správce front HA/DR a přesouvá se na jiný uzel, jeho stav HA je neznámý a jeho stav DR je neznámý. Chcete-li vyřešit toto selhání, musí být modul jádra DRBD aktualizován s cílem verze pro spuštěné jádro operačního systému.

```
Node:                                   main-alice
OS kernel version:                      3.10.0-1160.15.2
DRBD OS kernel version:                 3.10.0-957
DRBD version:                           9.1.2+ptf.3
DRBD kernel module status:              Partially loaded

Queue manager name:                     QM1
Queue manager status:                   Running elsewhere
HA status:                              Unknown
```

```
HA current location:                    main-bob
HA preferred location:                  This node
HA blocked location:                    None
DR role:                                Primary
DR status:                              Unknown
```

Související odkazy

Linux rdqmstatus

Linux *Provoz v prostředí DR/HA*

Při práci v prostředí DR/HA existují samostatné pokyny pro vysokou dostupnost a zotavení z havárie.

Pokud dojde k selhání uzlu, na kterém je spuštěn DR/HA RDQM, dojde k automatickému selhání RDQM na jiný uzel v této skupině HA. Pokud dojde k selhání celého serveru, musíte ručně spustit RDQM na upřednostňovaném uzlu ve skupině HA na serveru obnovy. Zde uvedené aspekty jsou stejné jako u běžného RDQM DR, další informace viz “Provoz v prostředí zotavení z havárie” na stránce 595 .

Pokud dojde k úplnému selhání jednoho z uzlů a je třeba jej nahradit, naleznete pokyny v části “Nahrazení uzlu, který selhal, v konfiguraci zotavení z havárie” na stránce 597 a “Nahrazení uzlu, u kterého došlo k selhání, v konfiguraci vysoké dostupnosti” na stránce 577 .

Linux *Nahrazení uzlu, který selhal, v konfiguraci DR/HA*

Pokud jeden z uzlů v jedné ze skupin HA selže, můžete jej nahradit.

Informace o této úloze

Postup se liší podle toho, zda je uzel, který nahrazujete, primární nebo sekundární v konfiguraci DR. V obou případech musí mít nový uzel identickou konfiguraci s uzlem, který nahrazujete, tj. musí mít stejný název hostitele, stejné adresy IP atd.

Můžete se také setkat se situací, kdy jste zcela ztratili skupinu HA na hlavním serveru nebo serveru obnovy a musíte nahradit celou skupinu HA.

Procedura

- V případě náhradního uzlu, který je primární v konfiguraci DR, postupujte na novém uzlu takto:
  a) Vytvořte soubor `rdqm.ini` , který odpovídá souborům na ostatních uzlech, a pak spusťte příkaz `rdqmadm -c` (viz “Definování klastru Pacemaker (skupina HA)” na stránce 554).
  b) Spusťte příkaz `crtmqm -sxs -rr p` *qmanager* , abyste znovu vytvořili každý DR/HA RDQM (viz “Vytváření DR/HA RDQMs” na stránce 603).
- V případě náhradního uzlu, který je v konfiguraci DR sekundární, postupujte na novém uzlu takto:
  a) Vytvořte soubor `rdqm.ini` , který odpovídá souborům na ostatních uzlech, a pak spusťte příkaz `rdqmadm -c` (viz “Definování klastru Pacemaker (skupina HA)” na stránce 554).
  b) Spusťte příkaz `crtmqm -sx -rr s` *qmanager* , abyste znovu vytvořili každý DR/HA RDQM (viz “Vytváření DR/HA RDQMs” na stránce 603).
- Chcete-li nahradit celou skupinu HA, postupujte takto:
  a) Pokud ztratíte celou skupinu HA na primárním serveru DR (tj. na hlavním serveru), musíte postupovat podle kroků, abyste provedli spravované překonání selhání na sekundárním serveru DR, abyste pokračovali v běhu modulů DR/HA RDQM (viz “Provoz v prostředí zotavení z havárie” na stránce 595). (Pokud ztratíte celou skupinu HA na místě obnovy, vaše DR/HA RDQM nadále běží na hlavním serveru bez vašeho zásahu.)
  b) Znovu vytvořte skupinu HA na vašich třech náhradních uzlech, jak je popsáno v tématu “Konfigurace skupin HA pro DR/HA RDQM” na stránce 602.
  c) Vytvořte znovu své RDQM DR/HA v nové skupině HA, jak je popsáno v tématu “Vytváření DR/HA RDQMs” na stránce 603.

d) V případě potřeby proveďte spravované překonání selhání ze serveru pro obnovu zpět na hlavní server.

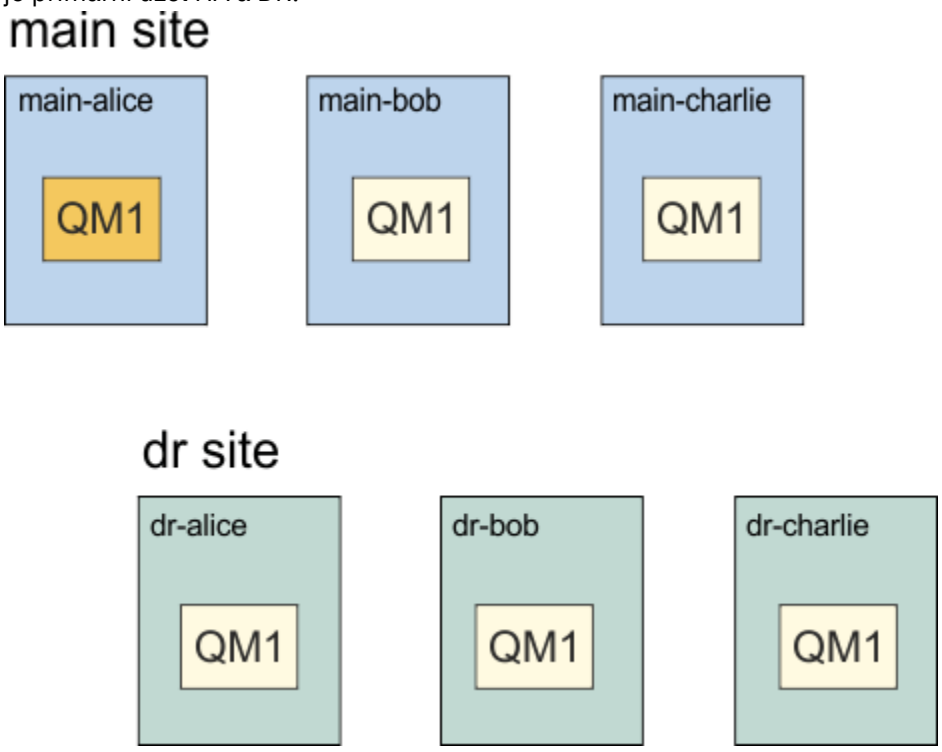
Linux *Příklad funkce DR/HA RDQM*

Tento příklad ukazuje, jak vytvořit a odstranit DR/HA RDQM.

Vytvoření DR/HA RDQM

Příklad konfigurace má dva servery s názvem 'main' a 'dr'. Každý server má tři uzly, nazvané 'alice', 'bob' a 'charlie'. Uzly mají úplný název skládající se z názvu serveru a názvu, takže 'main-alice', 'dr-alice' atd.

Následující kroky vytvoří DR/HA RDQM s názvem QM1 , který se spustí na hlavním-alice. Hlavní uzel alice je primární uzel HA a DR.



Pokud jsou v souboru `rdqm.ini` uvedeny lokální a vzdálené adresy IP DR, není třeba zadávat žádné adresy IP na příkazovém řádku a DR/HA RDQM s názvem QM1 lze vytvořit spuštěním následujícího příkazu na hlavním alice:

```
crtmqm -sx -rr p -rn DR1 -rp 7001 QM1
```

Pokud jsou adresy IP lokálního DR uvedeny v souboru `rdqm.ini` , pak mohou být adresy IP vzdáleného DR uvedeny na příkazovém řádku:

```
crtmqm -sx -rr p -ri 192.168.2.1,192.168.2.2,192.168.2.3 -rp 7001 QM1
```

Nejsou-li v souboru `rdqm.ini` uvedeny žádné adresy IP DR, mohou být na příkazovém řádku zadány adresy IP DR jak vzdálené, tak lokální:

```
crtmqm -sx -rr p -rl 192.168.1.1,192.168.1.2,192.168.1.3 -ri
192.168.2.1,192.168.2.2,192.168.2.3 -rp 7001 QM1
```

Výstup jako odpověď na vytvoření QM1 je uveden v následujícím příkladu:

```
Creating replicated data queue manager configuration.
Secondary queue manager created on 'main-bob'.
Secondary queue manager created on 'main-charlie'.
IBM MQ queue manager created.
Directory '/var/mqm/vols/qm1/qmgr/qm1' created.
```

```
The queue manager is associated with installation 'Installation1'.
Creating or replacing default objects for queue manager 'QM1'.
Default objects statistics : 83 created. 0 replaced. 0 failed.
Completing setup.
Setup completed.
Enabling replicated data queue manager.
Replicated data queue manager enabled.
Issue the following command on the remote HA group to create the DR/HA secondary queue manager:
crtmqm -sx -rr s -rl 192.168.2.1,192.168.2.2,192.168.2.3 -ri
192.168.1.1,192.168.1.2,192.168.1.3 -rp 7001 -fs 3072M QM1
```

Zkopírujte příkaz ze zprávy, abyste vytvořili sekundární instanci DR QM1 na dr-alice:

```
crtmqm -sx -rr s -rl 192.168.2.1,192.168.2.2,192.168.2.3 -ri
192.168.1.1,192.168.1.2,192.168.1.3 -rp 7001 -fs 3072M QM1
```

Následující zpráva je výstupem na dr-alice:

```
Creating replicated data queue manager configuration.
Secondary queue manager created on 'dr-bob'.
Secondary queue manager created on 'dr-charlie'.
IBM MQ secondary queue manager created.
Enabling replicated data queue manager.
```

Testovat sekundární DR

Chcete-li testovat funkce zotavení z havárie systému QM1, spusťte v hlavním alice následující příkaz, abyste QM1 učinili sekundární instancí DR:

```
rdqmdr -m QM1 -s
Queue manager 'QM1' has been made the DR secondary on this node.
```

Spusťte následující příkaz na dr-alice, abyste učinili QM1 primární instancí DR na tomto uzlu:

```
rdqmdr -m QM1 -p
Queue manager 'QM1' has been made the DR primary on this node.
```

Odstranění DR/HA RDQM

Chcete-li odstranit DR/HA RDQM s názvem QM1, nejprve ukončete správce front v hlavní oblasti:

```
endmqm -w QM1
Replicated data queue manager disabled.
Waiting for queue manager 'QM1' to end.
IBM MQ queue manager 'QM1' ended.
```

Pak spusťte následující příkaz na hlavním-alice, abyste odstranili QM1:

```
dltmqm QM1
Removing replicated data queue manager configuration.
Secondary queue manager deleted on 'main-bob'.
Secondary queue manager deleted on 'main-charlie'.
IBM MQ queue manager 'QM1' deleted.
```

Nakonec musíte odstranit QM1 na dr-alice:

```
dltmqm QM1
Removing replicated data queue manager configuration.
Secondary queue manager deleted on 'dr-bob'.
Secondary queue manager deleted on 'dr-charlie'.
IBM MQ queue manager 'QM1' deleted.
```

Související pojmy

“Provoz v prostředí DR/HA” na stránce 617

Při práci v prostředí DR/HA existují samostatné pokyny pro vysokou dostupnost a zotavení z havárie.

Související úlohy

“Vytváření DR/HA RDQMs” na stránce 603
Příkaz **crtmqm** se používá k vytvoření správce front replikovaných dat (RDQM) v konfiguraci DR/HA.

“Odstranění DR/HA RDQM” na stránce 607
Příkaz **dltmqm** se používá k odstranění správce front replikovaných dat DR/HA (RDQM).

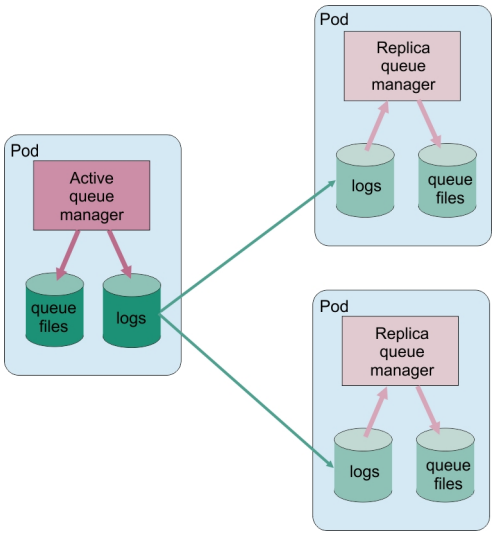
CP4I MQ Adv. Nativní vysoká dostupnost

Nativní HA je řešení vysoké dostupnosti, které je k dispozici na implementacích kontejnerů produktu IBM MQ.

Nativní konfigurace vysoké dostupnosti se skládá ze tří uzlů (které mohou být například tři sekce Kubernetes), z nichž každý má instanci správce front. Jedna instance je aktivní správce front, který zpracovává zprávy a zapisuje je do svého protokolu. Při každém zápisu protokolu odešle aktivní správce front data ostatním dvěma instancím označeným jako 'repliky'. Každá replika zapisuje do vlastního protokolu, potvrzuje data a poté aktualizuje vlastní data fronty z replikovaného protokolu. Pokud uzel, na kterém je spuštěn aktivní správce front, selže, jedna z instancí repliky správce front převezme aktivní roli a bude mít aktuální data, se kterou bude pracovat.

Podrobný přehled viz Nativní HA v sekci Kontejnery v této dokumentaci.

Na následujícím obrázku je znázorněna typická implementace se třemi instancemi správce front implementovaného ve třech kontejnerech.



Obrázek 83. Příklad konfigurace nativní vysoké dostupnosti

CP4I MQ Adv. *Vytvoření nativního řešení HA*

Doporučenou metodou pro vytvoření řešení nativní vysoké dostupnosti je použití IBM MQ Operator. Případně můžete vytvořit vlastní kontejnery a ručně nakonfigurovat nativní vysokou dostupnost.

Poznámka: Tyto informace platí pouze pro kontejnerová prostředí.

Chcete-li vytvořit řešení nativní vysoké dostupnosti pomocí konzoly IBM MQ Operator, prohlédněte si téma Nativní vysoká dostupnost , kde naleznete přehled a Příklad: Konfigurace správce front nativní vysoké dostupnosti , kde získáte podrobné pokyny.

Chcete-li vytvořit vlastní kontejnery a ručně nakonfigurovat nativní vysokou dostupnost, prohlédněte si téma Vytvoření skupiny nativní vysoké dostupnosti, pokud vytváříte vlastní kontejnery.

CP4I MQ Adv. *Ukončení nativních správců front HA*

Pro kontejnery IBM MQ můžete použít příkaz **endmqm** k ukončení aktivního nebo replikovaného správce front, který je součástí nativní skupiny HA.

Informace o této úloze

Poznámka: Tyto informace platí pouze pro kontejnerová prostředí.

Postup pro zastavení správce front, který je součástí nativní skupiny HA, závisí na tom, zda se jedná o aktivní instanci nebo instanci repliky. Když ukončíte kterýkoli typ instance, provede se kontrola, aby se zajistilo, že ukončení instance nepřeruší kvorum skupiny Nativní HA. Pokud by bylo kvorum přerušeno, příkaz **endmqm** se nezdaří.

Když zadáte příkaz **endmqm** , ostatní instance ve skupině budou varovány, že k tomu dochází, aby neohlašovaly chyby při přerušení připojení.

Pokud aktivní instance ztratí kvorum kvůli ukončení nebo odpojení příliš mnoha instancí repliky, čeká aktivní instance před úplným ukončením konfigurovatelnou dobu. To umožňuje časové období pro nenápadné ukončení zpracování, namísto toho, aby aplikace pouze přerušily svá připojení. Tuto hodnotu časového limitu může uvést atribut `QuorumConnectivityTimeout` v sekci `NativeHALocalInstance` souboru `qm.ini` . Výchozí hodnota je 0 sekund.

Procedura

- Chcete-li ukončit aktivní instanci správce front, zadejte v uzlu, v němž je aktivní instance spuštěna, následující příkaz:

  ```
  endmqm -s QMgrName
  ```

  – Zadejte volbu `-r` , která pomůže aplikacím klienta znovu se připojit k jiné instanci.
  – Pokud tato instance není aktivní instancí ve skupině Nativní HA, příkaz se nezdaří.
  – Pokud by ukončení této aktivní instance způsobilo selhání kvora skupiny, příkaz by selhal. (Pokud současně se spuštěním tohoto příkazu ukončí nebo se stanou nedostupnými jiné instance, nemusí to zjistit kontrola kvora, skupina Nativní HA skončí a může být restartována pouze tehdy, když je k dispozici dostatek instancí.)

  Po ukončení aktivního správce front převezme aktivní roli jedna z instancí repliky. Nemůžete určit, která replika převezme, to je určeno vyjednáváním v rámci skupiny a závisí na tom, který má nejaktuálnější transakční protokoly.
- Chcete-li ukončit instanci repliky správce front, zadejte následující příkaz:

  ```
  endmqm -x QMgrName
  ```

  – Pokud je tato instance aktivní instance, příkaz selže.
  – Pokud by ukončení této instance repliky způsobilo selhání kvora skupiny, příkaz by selhal. (Pokud současně se spuštěním tohoto příkazu ukončí nebo se stanou nedostupnými jiné instance, nemusí to zjistit kontrola kvora, skupina Nativní HA skončí a může být restartována pouze tehdy, když je k dispozici dostatek instancí.)

  Poznámka: Můžete také použít přepínače -c, -i, -p nebo -w s příkazem **endmqm** na nativních instancích HA, bez ohledu na to, ve které roli se nacházejí. Instance správce front bude ukončena a bude ignorován efekt, který má na kvorum skupiny. Informace jsou však stále sdíleny s ostatními instancemi ve skupině. Tyto přepínače můžete použít společně s parametrem -s pro aktivní instanci. Tyto přepínače nemůžete použít společně s přepínačem -x pro instance repliky.

Související odkazy
endmqm (koncový správce front)

Protokolování: Ujistěte se, že zprávy nejsou ztraceny

Produkt IBM MQ zaznamenává všechny významné změny trvalých dat řízených správcem front do protokolu pro zotavení.

To zahrnuje vytváření a odstraňování objektů, aktualizace trvalých zpráv, stavy transakcí, změny atributů objektů a aktivity kanálů. Protokol obsahuje informace, které potřebujete k obnově všech aktualizací front zpráv:

- Uchovávání záznamů o změnách správce front
- Uchovávání záznamů o aktualizacích fronty pro použití procesem restartování
- Umožnění obnovy dat po selhání hardwaru nebo softwaru

Produkt IBM MQ se však také spoléhá na diskový systém, který hostuje své soubory, včetně souborů protokolu. Pokud je diskový systém sám o sobě nespolehlivý, informace, včetně informací protokolu, mohou být stále ztraceny.

POZOR: Protokoly pro zotavení nelze přesunout do jiného operačního systému.

Jak vypadají protokoly

Protokoly se skládají z primárních a sekundárních souborů a řídicího souboru. Definujete počet a velikost souborů protokolu a jejich umístění v systému souborů.

Protokol IBM MQ se skládá ze dvou komponent:

1. Jeden nebo více souborů dat protokolu.
2. Řídicí soubor protokolu

Soubor dat protokolu je také znám jako oblast protokolu.

Existuje několik oblastí protokolu, které obsahují zaznamenávaná data. Můžete definovat počet a velikost (jak je vysvětleno v tématu “Sekce LogDefaults souboru mqs.ini” na stránce 93), nebo použít systémovou předvolbu tří primárních a dvou sekundárních oblastí.

Každá ze tří primárních a dvou sekundárních oblastí má výchozí hodnotu 16 MB.

Při vytváření správce front je počet předem přidělených oblastí protokolu počet *primárních* přidělených oblastí protokolu. Pokud neuvedete číslo, použije se výchozí hodnota.

Produkt IBM MQ používá dva typy protokolování:

- Kruhový
- Lineární

  Počet oblastí protokolu použitých s lineárním protokolováním může být velmi velký, v závislosti na frekvenci záznamu obrazu média.

Další informace viz “Typy protokolování” na stránce 623.

ALW Pokud jste v systémech IBM MQ for AIX or Linux nezměnili cestu k protokolu, jsou oblasti protokolu vytvořeny v adresáři:

```
/var/mqm/log/QMgrName
```

Windows Pokud jste v produktu IBM MQ for Windowsnezměnili cestu k protokolu, jsou oblasti protokolu vytvořeny v adresáři:

```
C:\ProgramData\IBM\MQ\log\QMgrName
```

Produkt IBM MQ začíná těmito oblastmi primárního protokolu, ale pokud není prostor primárního protokolu dostatečný, přidělí *sekundární* oblasti pro rozšíření protokolu. Provádí to dynamicky a odebírá je, když se sníží poptávka po protokolovacích prostorech. Standardně lze přidělit až dvě sekundární oblasti protokolu. Toto výchozí přidělení můžete změnit, jak je popsáno v tématu “Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83.

Oblasti protokolu mají předponu buď s písmenem S , nebo s písmenem R. Aktivní, neaktivní a nadbytečné fyzické oblasti mají předponu S, zatímco opětovné použití fyzických oblastí má předponu R.

Při zálohování nebo obnově správce front zálohujte a obnovte všechny aktivní, neaktivní a nadbytečné oblasti spolu s řídicím souborem protokolu.

Poznámka: Nemusíte zálohovat a obnovovat znovu použité oblasti pro rozšíření.

Řídicí soubor protokolu

Řídicí soubor protokolu obsahuje informace potřebné k popisu stavu fyzických oblastí protokolu, jako například jejich velikosti a umístění a názvu další dostupné oblasti.

Důležité: Soubor řízení protokolu je určen pouze pro interní správce front.

Správce front uchovává řídicí data přidružená ke stavu protokolu pro zotavení v řídicím souboru protokolu a vy nesmíte upravovat obsah řídicího souboru protokolu.

Řídicí soubor protokolu je v cestě k protokolu a nazývá se `amqhlctl.lfh`. Při zálohování nebo obnově správce front se ujistěte, že je řídicí soubor protokolu zálohován a obnoven spolu s oblastmi protokolu.

Typy protokolování

V produktu IBM MQ existují dva způsoby správy záznamů aktivit správce front: kruhové protokolování a lineární protokolování. Třetí typ protokolování, replikovaný, používají pouze nativní konfigurace vysoké dostupnosti.

Kruhové protokolování

Kruhové protokolování použijte, pokud vše, co chcete, je restartovat zotavení, pomocí protokolu k odvolání transakcí, které probíhaly při zastavení systému.

Kruhové protokolování zachová všechna data restartování v kruhu souborů protokolu. Protokolování vyplní první soubor v kruhu a poté vždy přejde na další, dokud nejsou naplněny všechny soubory. Nakonec přejde na první soubor v kruhu a začne znovu. Tento postup probíhá po celou dobu používání protokolu a má výhodu, že nikdy nedojde k nedostatku souborů protokolu.

Produkt IBM MQ uchovává položky protokolu potřebné k restartování správce front bez ztráty dat, dokud nejsou potřebné k zajištění obnovy dat správce front. Mechanizmus uvolnění souborů protokolu pro opětovné použití je popsán v části “Použití kontrolního bodu k zajištění úplné obnovy” na stránce 625.

lineární protokolování

Lineární protokolování použijte v případě, že chcete restartovat obnovu i obnovu médií (opětovné vytvoření ztracených nebo poškozených dat přehráním obsahu protokolu). Lineární protokolování uchovává data protokolu v souvislé posloupnosti souborů protokolu.

Soubory protokolu mohou být volitelně:

- Znovu použito, ale pouze v případě, že již nejsou potřebné pro obnovu po restartu nebo obnovu médií.
- Ručně archivováno pro dlouhodobé ukládání a analýzu.

Frekvence obrazů médií určuje, kdy lze znovu použít soubory lineárního protokolu, a je hlavním faktorem v tom, kolik místa na disku musí být k dispozici pro soubory lineárního protokolu.

Správce front můžete nakonfigurovat tak, aby automaticky pořizoval periodické obrazy médií na základě času nebo využití protokolu, nebo můžete obrazy médií naplánovat ručně.

Váš administrátor rozhodne, jakou zásadu implementovat, a důsledky na využití prostoru na disku. Soubory žurnálu potřebné pro obnovu po restartu musí být vždy k dispozici, zatímco soubory žurnálu potřebné pouze pro obnovu médií mohou být archivovány do dlouhodobého úložiště, například na pásku.

Pokud váš administrátor povolí automatickou správu protokolů a automatické obrazy médií, lineární protokolování se chová podobně jako velmi rozsáhlý kruhový protokol, ale se zlepšenou redundancí proti selhání médií povoleným obnovou médií.

V produktu IBM MQ 9.1.0 můžete změnit existující typ protokolu pro správce front z lineárního na kruhový nebo z kruhového na lineární pomocí příkazu migmqlog .

Replikované protokolování

CP4I

Ke konfiguraci nativní konfigurace vysoké dostupnosti použijte replikované protokolování. Při vytváření nativní skupiny HA vytvoříte tři správce front v různých uzlech. Zadejte typ protokolování replikovaný spolu s jedinečným názvem instance pro každého ze správců front. Nativní konfigurace vysoké dostupnosti poskytuje řešení vysoké dostupnosti tím, že má aktivní instanci replikovat data protokolu do dvou instancí repliky. Pokud se aktivní instance nezdaří, jedna z instancí repliky převezme aktivní roli. Replikace protokolu zajišťuje, že data budou ztracena jen velmi málo, pokud vůbec nějaká existují. Další podrobnosti viz “Nativní vysoká dostupnost” na stránce 620. Replikovaný protokol je ekvivalentní lineárnímu protokolu s povolenou automatickou správou protokolů a automatickými obrazy médií.

Oblasti lineárního protokolu, které nejsou aktivní

Multi

Pokud v produktu IBM MQ 9.1.0používáte automatickou správu protokolů, včetně archivace, zapisovač protokolu sleduje lineární oblasti protokolu, které nejsou aktivní.

Upozornění: Pokud používáte automatickou správu protokolů bez archivace, použití záložního správce front není pro tento proces podporováno.

ALW Pokud již není oblast protokolu potřebná pro obnovu a je-li to nutné, je archivována, modul protokolování v vhodném okamžiku buď odstraní oblast protokolu, nebo ji znovu použije.

Znovu použitá oblast pro rozšíření protokolu je přejmenována na další oblast v posloupnosti protokolu. Zpráva AMQ7490 se pravidelně zapisuje, což označuje, kolik oblastí bylo vytvořeno, odstraněno nebo znovu použito.

Modul protokolování zvolí, kolik oblastí pro rozšíření má být připraveno k opětovnému použití a kdy má být tato oblast odstraněna.

Aktivní protokol

Existuje řada souborů, které jsou v lineárním i kruhovém protokolování *aktivní* . Aktivní protokol je maximální množství protokolovacího prostoru, bez ohledu na to, zda používáte kruhové nebo lineární protokolování, na které může odkazovat zotavení po restartu.

Počet aktivních souborů protokolu je obvykle menší než počet primárních souborů protokolu, jak je definováno v konfiguračních souborech. (Informace o definování čísla naleznete v části “Výpočet velikosti protokolu” na stránce 628 .)

Všimněte si, že aktivní protokolovací prostor nezahrnuje prostor požadovaný pro obnovu médií a že počet souborů protokolu použitých s lineárním protokolováním může být velmi velký, v závislosti na toku zpráv a frekvenci obrazů médií.

Neaktivní protokol

Když již není soubor protokolu potřebný pro zotavení po restartu, stane se *neaktivním*. Soubory protokolu, které nejsou vyžadovány pro zotavení při restartu nebo zotavení z média, lze považovat za nadbytečné soubory protokolu.

Při použití automatické správy protokolů správce front řídí zpracování těchto nadbytečných souborů protokolu. Pokud jste vybrali ruční správu protokolů, je povinností administrátora spravovat (například odstranit a archivovat) nadbytečné soubory protokolů, pokud již nejsou pro vaši operaci zajímavé.

Další informace o dispozici souborů protokolu naleznete v tématu “Správa protokolů” na stránce 634 .

Sekundární soubory protokolu

Ačkoli jsou sekundární soubory protokolu definovány pro lineární protokolování, nepoužívají se v normálním provozu. Pokud nastane situace, kdy pravděpodobně kvůli dlouho trvajícím transakcím není možné uvolnit soubor z aktivního fondu, protože může být stále požadován pro restart, sekundární soubory jsou formátovány a přidány do aktivního fondu souborů protokolu.

Pokud je počet dostupných sekundárních souborů využit, požadavky na většinu dalších operací, které vyžadují aktivitu protokolu, budou odmítnuty s návratovým kódem MQRC_RESOURCE_PROBLEM vráceným aplikaci a všechny dlouho běžící transakce budou zvažovány pro asynchronní odvolání.

Upozornění: Všechny typy protokolování se mohou vyrovnat s neočekávanou ztrátou napájení, za předpokladu, že nedochází k selhání hardwaru.

Použití kontrolního bodu k zajištění úplné obnovy

Kruhové protokolování i správci front s lineárním protokolováním podporují zotavení při restartu. Bez ohledu na to, jak náhle se předchozí instance správce front ukončí (například výpadek proudu) po restartování správce front obnoví svůj trvalý stav do správného transakčního stavu v okamžiku ukončení.

Obnova při restartu závisí na zachování integrity disku. Podobně by měl operační systém zajistit integritu disku bez ohledu na to, jak náhle může dojít k ukončení operačního systému.

Ve velmi neobvyklé události, že integrita disku není udržována, pak lineární protokolování (a obnova médií) poskytuje některé další možnosti redundance a obnovitelnosti. Díky stále běžnějším technologiím, jako je RAID, je stále vzácnější trpět problémy s integritou disku a mnoho podniků konfiguruje kruhové protokolování a používá pouze restartovat zotavení.

Produkt IBM MQ je navržen jako klasický správce prostředků protokolování přímého zápisu. Trvalé aktualizace front zpráv se provádějí ve dvou fázích:

1. Záznamy protokolu reprezentující aktualizaci jsou spolehlivě zapsány do protokolu pro zotavení.
2. Soubor nebo vyrovnávací paměti fronty jsou aktualizovány způsobem, který je pro váš systém nejefektivnější, ale ne nutně konzistentně.

Soubory protokolu tak mohou být více aktuální než základní vyrovnávací paměť fronty a stav souboru.

Pokud bylo povoleno, aby tato situace pokračovala nezmenšená, bude po zotavení z havárie vyžadován velmi velký objem přehrání protokolu, aby byl stav fronty konzistentní.

Produkt IBM MQ používá produkt `checkpoints` k omezení objemu přehrání protokolu vyžadovaného po zotavení z havárie. Klíčová událost, která řídí, zda je soubor protokolu označován jako aktivní, či nikoli, je `checkpoint`.

Kontrolní bod IBM MQ je bod:

- Konzistence mezi protokolem pro zotavení a soubory objektů.
- To identifikuje místo v protokolu, z něhož je zaručeno, že dopředné přehrání následných záznamů protokolu obnoví frontu do správného logického stavu v době, kdy mohl být správce front ukončen.

Během kontrolního bodu produkt IBM MQ podle potřeby vyprazdňuje starší aktualizace souborů front, aby omezil objem záznamů protokolu, které je třeba přehrát, aby se fronty vrátily do konzistentního stavu po zotavení z havárie.

Poslední dokončený kontrolní bod označuje bod v protokolu, ze kterého musí být přehrání provedeno během zotavení z havárie. Frekvence kontrolního bodu je tedy kompromisem mezi režií zaznamenávání kontrolních bodů a zlepšením potenciální doby obnovy, kterou tyto kontrolní body předpokládají.

V produktu IBM MQ 9.1.0modul protokolování plánuje kontrolní body častěji (takže další je naplánován před dokončením předchozího), protože se modul protokolování pokouší uchovat aktivní protokol v primárních oblastech protokolu. Pokud to není možné, zaprotokoluje se chyba AMQ7466 .

Pozice v protokolu začátku nejnovějšího dokončeného kontrolního bodu je jedním z klíčových faktorů při určování, zda je soubor protokolu aktivní nebo neaktivní. Dalším klíčovým faktorem je pozice v protokolu prvního záznamu protokolu týkající se první trvalé aktualizace provedené aktuální aktivní transakcí.

Pokud je nový kontrolní bod zaznamenán ve druhém nebo pozdějším, soubor protokolu a žádná aktuální transakce se neodkazuje na záznam protokolu v prvním souboru protokolu, první soubor protokolu se stane neaktivním. V případě kruhového protokolování je nyní první soubor protokolu připraven k opětovnému použití. V případě lineárního protokolování bude první soubor protokolu obvykle stále vyžadován pro obnovu médií.

Pokud konfigurujete kruhové protokolování nebo automatickou správu protokolů, správce front bude spravovat neaktivní soubory protokolu. Pokud nakonfigurujete lineární protokolování s ruční správou protokolů, stane se administrativní úlohou pro správu neaktivních souborů podle požadavků vaší operace.

Produkt IBM MQ generuje kontrolní body automaticky. Jsou užívány v následujících časech:

- Při spuštění správce front
- Při ukončení práce systému
- Když je protokolovací prostor nízký
- Multi Poté, co bylo od předchozího kontrolního bodu zaprotokolováno 50 000 operací
- z/OS Po zaprotokolování *number_of_operations* od předchozího kontrolního bodu, kde *number_of_operations* je počet operací nastavených ve vlastnosti **LOGLOAD** .

Když se produkt IBM MQ restartuje, vyhledá nejnovější záznam kontrolního bodu v protokolu. Tyto informace jsou uloženy v souboru kontrolních bodů, který je aktualizován na konci každého kontrolního bodu. Všechny operace, které proběhly od kontrolního bodu, jsou přehrávány vpřed. Toto je známé jako fáze přehrání.

Fáze přehrání vrátí fronty zpět do logického stavu, ve kterém se nacházely před selháním systému nebo před ukončením práce systému. Během fáze přehrání se vytvoří seznam transakcí, které probíhaly v době, kdy došlo k selhání systému nebo k ukončení práce systému.

Multi Jsou vydány zprávy AMQ7229 a AMQ7230 , které označují průběh fáze přehrání.

Chcete-li vědět, které operace se mají vrátit zpět nebo potvrdit, produkt IBM MQ přistupuje ke každému záznamu aktivního protokolu přidruženému k probíhající transakci. Toto je známé jako fáze obnovy.

Multi Jsou vydány zprávy AMQ7231, AMQ7232 a AMQ7234 , které označují průběh fáze obnovy.

Po přístupu ke všem nezbytným záznamům protokolu během fáze zotavení je každá aktivní transakce postupně vyřešena a každá operace přidružená k transakci bude buď vrácena zpět, nebo potvrzena. Toto je známé jako fáze řešení.

Multi Je vydána zpráva AMQ7233 , která označuje průběh fáze řešení.

z/OS V systému z/OSse zpracování restartu skládá z různých fází.

1. Rozsah protokolu pro zotavení je vytvořen na základě zotavení médií vyžadovaného pro sady stránek a nejstaršího záznamu protokolu, který je nezbytný pro zálohování jednotek práce a získání zámků pro neověřené jednotky práce.
2. Jakmile je určen rozsah protokolu, provede se dopředný odečet protokolu, aby se nastavení stránky převedlo do nejnovějšího stavu, a také se zamknou všechny zprávy, které se týkají nejistých nebo probíhajících pracovních jednotek.
3. Po dokončení dopředného čtení protokolu jsou protokoly čteny dozadu, aby se všechny jednotky práce, které byly v době selhání v průběhu nebo v době vrácení zpět, stály zpět.

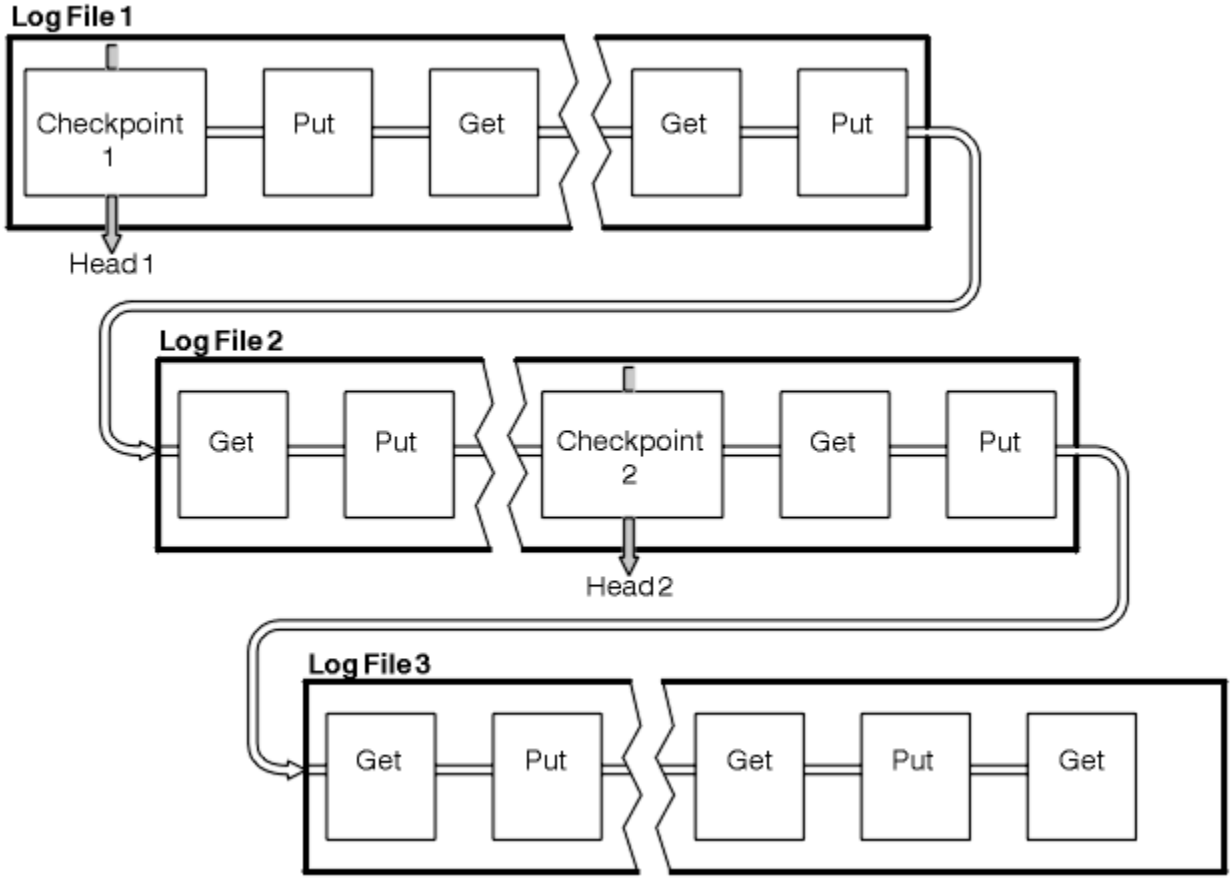
z/OS Příklad zpráv, které můžete vidět:

```
CSQR001I +MQOX RESTART INITIATED
CSQR003I +MQOX RESTART - PRIOR CHECKPOINT RBA=00000001E48C0A5E
CSQR004I +MQOX RESTART - UR COUNTS -  806
IN COMMIT=0, INDOUBT=0, INFLIGHT=0, IN BACKOUT=0
CSQR030I +MQOX Forward recovery log range  815
from RBA=00000001E45FF7AD to RBA=00000001E48C1882
```

```
CSQR005I +MQOX RESTART - FORWARD RECOVERY COMPLETE -  816
IN COMMIT=0, INDOUBT=0
CSQR032I +MQOX Backward recovery log range  817
from RBA=00000001E48C1882 to RBA=00000001E48C1882
CSQR006I +MQOX RESTART - BACKWARD RECOVERY COMPLETE -  818
INFLIGHT=0, IN BACKOUT=0
CSQR002I +MQOX RESTART COMPLETED
```

Poznámka: Je-li k dispozici velké množství protokolu ke čtení, jsou pravidelně vydávány zprávy CSQR031I (dopředná obnova) a CSQR033I (zpětná obnova), které zobrazují průběh.

V produktu Obrázek 84 na stránce 627již produkt IBM MQnepotřebuje všechny záznamy před posledním kontrolním bodem, kontrolním bodem 2. Fronty lze obnovit z informací o kontrolních bodech a z dalších záznamů protokolu. Pro kruhové protokolování lze znovu použít všechny uvolněné soubory před kontrolním bodem. V případě lineárního protokolu již uvolněné soubory protokolu nemusí být přístupné pro normální provoz a stanou se neaktivními. V tomto příkladu je ukazatel na záhlaví fronty přesunut tak, aby ukazoval na nejnovější kontrolní bod, kontrolní bod 2, který se pak stane novým hlavním bodem fronty, Hlava 2. Soubor protokolu 1 lze nyní znovu použít.



Obrázek 84. Kontrolní stanoviště

Kontrola pomocí přerušitelných transakcí

Jak dlouho běžící transakce ovlivňuje opětovné použití souborů protokolu.

Obrázek 85 na stránce 628 ukazuje, jak přerušitelná transakce ovlivňuje opětovné použití souborů protokolu. V tomto příkladu provedla přerušitelná transakce záznam do protokolu, zobrazený jako LR 1, po prvním zobrazeném kontrolním bodu. Transakce se nedokončí (v bodě LR 2), dokud neskončí třetí kontrolní bod. Všechny informace protokolu od LR 1 dále jsou uchovány, aby v případě potřeby umožnily obnovu této transakce, dokud nebude dokončena.

Po dokončení dlouhotrvající transakce, na LR 2, se hlavička protokolu logicky přesune na kontrolní bod 3, nejnovější protokolovaný kontrolní bod. Soubory obsahující záznamy protokolu před kontrolním bodem 3, hlavou 2, již nejsou potřeba. Pokud používáte kruhové protokolování, prostor lze znovu použít.

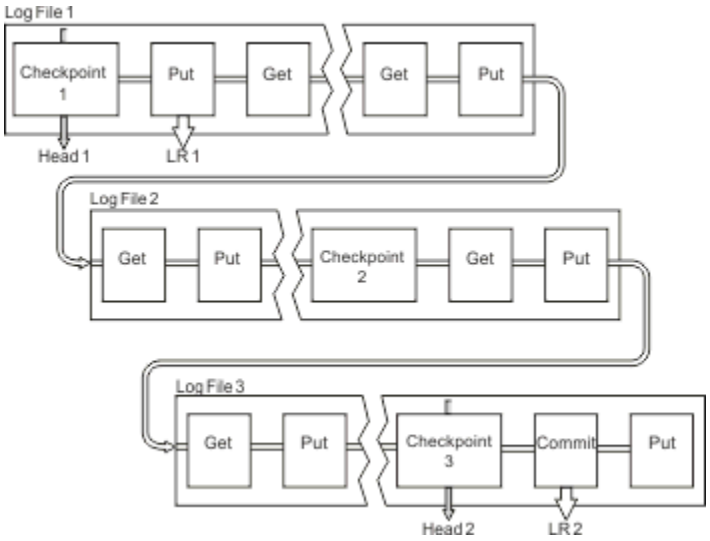
Pokud jsou primární soubory protokolu před dokončením přerušitelné transakce zcela zaplněny, mohou být použity sekundární soubory protokolu, aby se zabránilo zaplnění protokolů.

Aktivity, které jsou zcela pod kontrolou správce front, například kontrola průběžného stavu, jsou naplánovány tak, aby se pokusily udržet aktivitu v primárním protokolu.

Je-li však vyžadován sekundární protokolovací prostor pro podporu chování mimo řízení správce front (například doba trvání jedné z vašich transakcí), pokusí se správce front o použití libovolného definovaného sekundárního protokolovacího prostoru, aby bylo možné tuto aktivitu dokončit.

Pokud se tato aktivita nedokončí v době, kdy se používá 80% celkového protokolovacího prostoru, správce front zahájí akci uvolnění protokolovacího prostoru bez ohledu na skutečnost, že to má vliv na aplikaci.

Když je hlavička protokolu přesunuta a používáte kruhové protokolování, primární soubory protokolu se mohou stát vhodnými pro opětovné použití a modul protokolování po vyplnění aktuálního souboru znovu použije první primární soubor, který má k dispozici. Pokud používáte lineární protokolování, hlavička protokolu se stále přesune dolů v aktivním fondu a první soubor se stane neaktivním. Nový primární soubor je naformátován a přidán do spodní části fondu v připravenosti pro budoucí aktivity protokolování.



Obrázek 85. Kontrolní stanoviště s přerušitelnou transakcí

Výpočet velikosti protokolu

Odhad velikosti protokolu, který správce front potřebuje.

Po rozhodnutí, zda správce front používá kruhové nebo lineární protokolování, je třeba odhadnout velikost aktivního protokolu , který správce front potřebuje. Velikost aktivního protokolu je určena následujícími konfiguračními parametry protokolu:

LogFilePages
Velikost každého primárního a sekundárního souboru protokolu v jednotkách stránek 4K

LogPrimaryFiles
Počet předem přidělených primárních souborů protokolu

LogSecondaryFiles
Počet sekundárních souborů protokolu, které lze vytvořit pro použití při zaplnění primárních souborů protokolu

Notes:

1. Počet primárních a sekundárních souborů protokolu můžete změnit při každém spuštění správce front, i když si nemusíte všimnout vlivu změny, kterou provedete v sekundárních protokolech okamžitě.
2. Velikost souboru protokolu nelze změnit; musíte ji určit **před** vytvořením správce front.

3. Počet primárních souborů protokolu a velikost souboru protokolu určují velikost protokolovacího prostoru, který je předem přidělen při vytvoření správce front.
4. Celkový počet primárních a sekundárních souborů protokolu nemůže v systémech AIX and Linux překročit 511 nebo 255 v systému Windows, což v přítomnosti přerušitelných transakcí omezuje maximální množství prostoru pro žurnál, který je k dispozici správci front pro zotavení po restartu. Velikost protokolovacího prostoru, který může správce front potřebovat pro zotavení z médií, tento limit nesdílí.
5. Při použití *kruhového* protokolování správce front znovu použije primární a sekundární protokolovací prostor. Správce front přidělí až do limitu sekundární soubor protokolu, jakmile se soubor protokolu zaplní, a další primární soubor protokolu v posloupnosti nebude k dispozici.

   Informace o počtu protokolů, které potřebujete přidělit, naleznete v části "Jak velký bych měl (a) vytvořit aktivní protokol?" na stránce 629 . Primární oblasti žurnálu se používají v posloupnosti a tato posloupnost se nemění.

   Máte-li například tři primární protokoly `0`, `1`a `2`, pořadí použití je `0`,`1`,`2` následované `1`,`2`,`0`, `2`,`0`,`1`, zpět na `0`,`1`,`2` atd. Všechny sekundární protokoly, které jste přidělili, jsou podle potřeby proloženy.
6. Primární soubory protokolu jsou zpřístupněny pro opětovné použití během kontrolního bodu. Správce front vezme v úvahu jak primární, tak sekundární protokolovací prostor, než vezme kontrolní bod, protože velikost protokolovacího prostoru je nízká.

   Správce front se pokusí naplánovat kontrolní body způsobem, který uchová využití protokolu v rámci primárních oblastí.

Další informace viz "Sekce LogDefaults souboru mqs.ini" na stránce 93.

Jak velký bych měl (a) vytvořit aktivní protokol?

Odhad velikosti aktivního protokolu, který správce front potřebuje.

Velikost aktivního protokolu je omezena:

```
logsize = (primaryfiles + secondaryfiles) * logfilepages * 4096
```

Protokol by měl být dostatečně velký, aby se vypořádal s nejdéle běžící transakcí spuštěnou, když správce front zapisuje maximální množství dat za sekundu na disk.

Pokud je vaše nejdéle běžící transakce spuštěna po dobu `N` sekund a maximální množství dat za sekundu zapsaných na disk správcem front je `B` bajtů za sekundu v protokolu, váš protokol by měl být alespoň:

```
logsize >= 2 * (N+1) * B
```

Správce front pravděpodobně zapisuje maximální množství dat za sekundu na disk, když pracujete ve špičce pracovní zátěže, nebo když zaznamenáváte obrazy médií.

Pokud je transakce spuštěna tak dlouho, že oblast protokolu obsahující první záznam protokolu není obsažena v aktivním protokolu, správce front postupně odvolá aktivní transakce, počínaje transakcí s nejstarším záznamem protokolu.

Správce front musí před použitím maximálního počtu primárních a sekundárních souborů deaktivovat staré oblasti protokolu a správce front musí přidělit jinou oblast protokolu.

Rozhodněte, jak dlouho chcete spustit nejdéle běžící transakci, než ji bude moci správce front odvolat. Nejdéle běžící transakce může čekat na pomalý síťový provoz nebo, v případě špatně navržené transakce, na vstup uživatele.

Zadáním následujícího příkazu **runmqsc** můžete zjistit, jak dlouho nejdéle běžící transakce běží:

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

Zadáním příkazu `dspmqtrn -a` zobrazíte všechny příkazy XA a jiné než XA ve všech stavech.

Zadáním tohoto příkazu vypíše datum a čas, kdy byl zapsán první záznam protokolu pro všechny vaše aktuální transakce.

Upozornění: Pro účely výpočtu velikosti protokolu je důležitý čas od zápisu prvního záznamu protokolu, nikoli čas od spuštění aplikace nebo transakce. Zaokrouhlit délku nejdéle běžící transakce na nejbližší sekundu. Důvodem jsou optimalizace ve správci front.

První záznam protokolu lze zapsat dlouho po spuštění aplikace, pokud aplikace začíná například vyvoláním volání MQGET, které před skutečným získáním zprávy čeká určitou dobu.

Přezkoumáním maximálního pozorovaného data a času výstupu z

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

původně vydaný příkaz, od aktuálního data a času, můžete odhadnout, jak dlouho bude nejdéle běžící transakce spuštěna.

Ujistěte se, že tento příkaz **runmqsc** spouštíte opakovaně, zatímco nejdéle běžící transakce běží ve špičce pracovní zátěže, abyste nepodcenili délku nejdéle běžící transakce.

V produktu IBM MQ 8.0 použijte nástroje operačního systému, například **iostat** na platformách UNIX .

V produktu IBM MQ 9.0můžete zjistit bajty za sekundu, které správce front zapisuje do protokolu, zadáním následujícího příkazu:

```
amqsrua -m qmgr -c DISK -t Log
```

Zapsané logické bajty zobrazují bajty za sekundu, které správce front zapisuje do protokolu. Příklad:

```
$ amqsrua -m mark -c DISK -t Log
Publication received PutDate:20160920 PutTime:15383157 Interval:4 minutes,39.579 seconds
Log - bytes in use 37748736
Log - bytes max 50331648
Log file system - bytes in use 316243968
Log file system - bytes max 5368709120
Log - physical bytes written 4334030848 15501948/sec
Log - logical bytes written 3567624710 12760669/sec
Log - write latency 411 uSec
```

V tomto příkladu jsou logické bajty za sekundu zapsané do protokolu 12760669/sec nebo přibližně 12 MiB za sekundu.

Použití produktu

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

ukázal, že nejdéle běžící transakce byla:

```
CONN(57E14F6820700069)
EXTCONN(414D51436D61726B2020202020202020)
TYPE(CONN)
APPLTAG(msginteg_r)                     UOWLOGDA(2016-09-20)
UOWLOGTI(16.44.14)
```

Vzhledem k tomu, že aktuální datum a čas byl 2016-09-20 16.44.19, tato transakce byla spuštěna po dobu 5 sekund. Vyžadujete však toleranci transakcí spuštěných po dobu 10 sekund, než je správce front odvolá. Takže vaše velikost protokolu by měla být:

```
2 * (10 + 1) * 12 = 264 MiB
```

.

Počet souborů protokolu musí být schopen obsahovat největší očekávanou velikost protokolu (vypočtenou v předchozím textu). Jedná se o:

Minimální počet souborů protokolu = (Požadovaná velikost protokolu)/(**LogFilePages** * velikost stránky souboru protokolu (4096))

Při použití výchozího parametru **LogFilePages**, který je 4096, a odhadu velikosti protokolu 264MiB, vypočteného v předchozím textu, by měl být minimální počet souborů protokolu:

```
264MiB / (4096 x 4096) = 16.5
```

to znamená, že 17 souborů protokolu.

Pokud velikost protokolu odpovídá očekávané pracovní zátěži spuštěné v primárních souborech, postupujte takto:

- Sekundární soubory poskytují určitou nepředvídavost v případě, že je zapotřebí další protokolovací prostor.
- Kruhové protokolování vždy používá předalokované primární soubory, což je nepatrně rychlejší než alokace a dealokace sekundárních souborů.
- Správce front používá k výpočtu, kdy má provést další kontrolní bod, pouze zbývající prostor v primárních souborech.

Proto v předchozím příkladu nastavte následující hodnoty, aby se pracovní zátěž spustila v primárních souborech protokolu:

- **LogFilePages** = 4096
- **LogPrimaryFiles** = 17
- **LogSecondaryFiles** = 5

Všimněte si následujícího:

- V tomto příkladu je 5 sekundárních logů více než 20% aktivního protokolovacího prostoru.

  Z produktu IBM MQ 9.1.0se modul protokolování pokusí udržet pracovní zátěž v primárních souborech o samotě. Proto modul protokolování plánuje kontrolní body, když je plný pouze zlomek primárních souborů.

  Mít sekundární soubory je nepředvídaná situace, v případě, že existují nějaké neočekávaně dlouho běžící transakce.

  Měli byste si uvědomit, že správce front provede akci ke snížení využití protokolovacího prostoru, když se používá více než 80% celkového protokolovacího prostoru.
- Proveďte stejný výpočet bez ohledu na to, zda používáte lineární nebo kruhové protokolování.

  Nezáleží na tom, zda vypočítáváte velikost lineárního nebo kruhového aktivního protokolu, protože koncept aktivního protokolu znamená totéž jak v lineárním protokolování, tak v kruhovém protokolování.
- Oblasti protokolu potřebné pouze pro obnovu médií nejsou v aktivním protokolu, a proto nejsou započítány do počtu primárních a sekundárních souborů.
- Z IBM MQ 9.1.0 pole *LOGUTIL* DISPLAY QMSTATUS LOG je k dispozici pro výpočet přibližně požadované velikosti aktivního protokolu.

  Toto pole je navrženo tak, aby vám umožnilo provést přiměřený odhad požadované velikosti protokolu bez neustálého vzorkování, aby bylo možné určit dobu trvání nejdéle běžících transakcí nebo maximální propustnost správce front.

Jak velké by měly být stránky LogFile?

Obecně nastavte stránky LogFiledostatečně velké, aby bylo možné snadno zvětšit velikost aktivního protokolu bez dosažení maximálního počtu primárních souborů. Několik velkých souborů protokolu je vhodnější než mnoho malých souborů protokolu, protože několik velkých souborů protokolu vám umožňuje větší flexibilitu při zvyšování velikosti protokolu, pokud to potřebujete.

V případě lineárního protokolování mohou velmi velké soubory protokolu vytvořit proměnnou výkonu. U velmi velkých souborů protokolu je větší krok k vytvoření a formátování nového souboru protokolu nebo k archivaci starého. Jedná se spíše o problém s ruční a archivační správou protokolů, protože s automatickou správou protokolů se zřídka vytvářejí nové soubory protokolů.

Co se stane, když udělám svůj protokol příliš malý?

Body, které musíte zvážit při odhadování minimální velikosti protokolu.

Pokud je váš protokol příliš malý:

- Dlouho běžící transakce budou vráceny zpět.
- Další kontrolní bod chce začít před ukončením předchozího kontrolního bodu.

Důležité: Bez ohledu na to, jak nepřesně odhadujete velikost protokolu, je zachována integrita dat.

Vysvětlení kontrolních bodů naleznete v části "Použití kontrolního bodu k zajištění úplné obnovy" na stránce 625 . Pokud velikost prostoru pro žurnál, který zbývá v oblastech aktivního protokolu, začíná být krátká, správce front naplánuje kontrolní body častěji.

Kontrolní bod trvá určitou dobu; není okamžitý. Čím více dat je třeba zaznamenat do kontrolního bodu, tím déle bude kontrolní bod trvat. Pokud je protokol malý, kontrolní body se mohou překrývat, což znamená, že další kontrolní bod je požadován před ukončením předchozího kontrolního bodu. Pokud k tomu dojde, jsou zapsány chybové zprávy.

Pokud dojde k vrácení dlouho běžících transakcí nebo k překrytí kontrolních bodů, bude správce front pokračovat ve zpracování pracovní zátěže. Krátkodobé transakce pokračují v normální činnosti.

Správce front však není spuštěn optimálně a výkon může být snížen. Měli byste restartovat správce front s dostatečným prostorem pro žurnál.

Co se stane, když udělám svůj protokol příliš velký?

Body, které musíte zvážit při odhadování maximální velikosti protokolu.

Pokud je váš protokol příliš velký:

- Můžete zvýšit dobu potřebnou pro nouzové restartování, i když je to nepravděpodobné.
- Používáte nepotřebný prostor na disku.
- Velmi dlouho běžící transakce jsou tolerovány.

Důležité: Bez ohledu na to, jak nepřesně odhadujete velikost protokolu, je zachována integrita dat.

Chcete-li pomoci odhadnout maximální velikost protokolu, můžete použít statistiku využití protokolu. Další informace viz "Rozhodování o tom, jak nastavit IMGLOGLN a IMGINTVL" na stránce 638 a ALTER QMGR.

Popis způsobu, jakým správce front čte protokol při restartu, naleznete v části "Použití kontrolního bodu k zajištění úplné obnovy" na stránce 625 . Správce front přehraje protokol z posledního kontrolního bodu a poté vyřeší všechny transakce, které byly aktivní po ukončení správce front.

Chcete-li vyřešit transakci, správce front načte zpět všechny záznamy protokolu přidružené k této transakci. Tyto záznamy protokolu mohou být před posledním kontrolním bodem.

Přidělením velmi velkého protokolu správci front dáváte správci front oprávnění ke čtení všech záznamů protokolu při restartu, ačkoli obvykle to správce front nemusí provádět. Potenciálně, v nepravděpodobném případě, že k tomu dojde, může tento proces trvat dlouho.

Pokud došlo k neočekávanému zastavení kontrolního bodu před ukončením správce front, dojde k výraznému zvýšení doby restartování pro správce front s rozsáhlým protokolem. Omezení velikosti protokolu omezuje dobu nouzového restartu.

Chcete-li se vyhnout těmto problémům, měli byste se ujistit, že:

- Pracovní zátěž se pohodlně vejde do protokolu, který není příliš velký.
- Vyhnete se dlouho běžícím transakcím.

Jak velký by měl být souborový systém protokolu?

Odhad velikosti systému souborů protokolu, který správce front potřebuje.

Je důležité, aby byl systém souborů protokolu dostatečně velký, aby měl váš správce front dostatek místa pro zápis svého protokolu. Pokud správce front zcela zaplní systém souborů protokolu, zapíše data FFDC, odvolá transakce a může správce front náhle ukončit.

Množství místa na disku, které rezervujete pro protokol, musí být alespoň tak velké jako aktivní protokol. Přesně to, kolik větší závisí na:

- Váš výběr typu protokolu (lineární nebo kruhový)
- Velikost aktivního protokolu (primární soubory, sekundární soubory, stránky souboru protokolu)
- Vaše volba správy protokolů (ruční, automatické nebo archivní)
- Vaše pohotovostní plány v případě poškozeného objektu.

Pokud zvolíte cyklický protokol, systém souborů protokolu by měl být

```
LogFilesystemSize >= (PrimaryFiles + SecondaryFiles + 1) * LogFileSize
```

To umožňuje správci front zapisovat do všech primárních a sekundárních souborů. Ve výjimečných případech může správce front zapsat další oblast nad počet sekundárních oblastí. Předchozí algoritmus to bere v úvahu.

Pokud zvolíte lineární protokol, systém souborů protokolu by měl být výrazně větší než aktivní protokol.

Zvolíte-li ruční správu protokolů, bude správce front pokračovat v zápisu do nových oblastí protokolu, jak je potřebuje, a je vaší odpovědností je odstranit (a archivovat je), pokud již nejsou zapotřebí.

O kolik větší musí být systém souborů protokolu, závisí do značné míry na vaší strategii odstraňování nadbytečných nebo neaktivních oblastí.

Můžete se rozhodnout archivovat a odstranit oblasti, jakmile se stanou neaktivními (nepotřebné pro obnovu po restartu), nebo se můžete rozhodnout archivovat a odstranit pouze nadbytečné oblasti (nepotřebné pro obnovu média nebo pro obnovu po restartu).

Pokud archivujete a odstraňujete pouze nadbytečné oblasti a pokud máte poškozený objekt, **MEDIALOG** se nepohne vpřed, takže žádné další oblasti nebudou nadbytečné. Archivování a odstraňování oblastí bude zastaveno, dokud problém nevyřešíte, například obnovením objektu.

Pokud pracovní zátěž nezastavíte, doba, po kterou budete muset problém vyřešit, závisí na velikosti systému souborů protokolu. Proto je doporučeným postupem mít při použití lineárního protokolování velkorysý systém souborů protokolu.

Vyberete-li lineární protokol a automatickou správu nebo správu archivního protokolu, správce front znovu použije oblasti protokolu.

Oblasti protokolu, které jsou k dispozici pro opětovné použití, mají předponu s písmenem R. Je-li zaznamenán obraz média a jsou-li archivovány nadbytečné fyzické oblasti, může správce front tyto fyzické oblasti znovu použít.

Opětovné použití oblastí pro rozšíření je tedy menší než délka dat zapsaných do protokolu mezi obrazy médií:

```
ReuseExtents <= LogDataLengthBetweenMediaImages
```

Při automatickém záznamu obrazů médií a nastavení **IMGLOGLN**může být hodnota `LogDataLengthBetweenMediaImages` až dvakrát **IMGLOGLN** , protože **IMGLOGLN** není cílem pevného maxima.

Při ručním záznamu obrazů médií nebo jejich automatickém záznamu podle intervalu závisí produkt `LogDataLengthBetweenMediaImages` na pracovní zátěži a intervalu mezi pořizováním obrazů.

Kromě aktivních oblastí pro rozšíření a opětného použití oblastí pro rozšíření existují neaktivní oblasti pro rozšíření (potřebné pouze pro obnovu médií) a nadbytečné oblasti pro rozšíření (nepotřebné pro restart nebo obnovu médií).

Při použití automatické správy protokolů nebo správy archivů správce front znovu nevyužívá oblasti potřebné pro zotavení z médií. Počet neaktivních oblastí tedy závisí na tom, jak často pořizujete obrazy médií a zda je pořizujete ručně nebo automaticky.

IMGINTVL a **IMGLOGLN** jsou cíle, nikoli pevné minimum nebo maximum mezi obrazy médií. Avšak při odhadování maximální velikosti systému souborů protokolu, kterou budete potřebovat, je nepravděpodobné, že by automatické obrazy médií byly zaznamenány více než dvakrát **IMGINTVL** nebo **IMGLOGLN** odděleně.

Při určování velikosti souborového systému protokolu pomocí automatické správy nebo správy protokolu archivace byste měli také zvážit, co se může stát v případě, že je fronta nebo jiný objekt poškozen. V takovém případě není správce front schopen pořídit obraz média poškozeného objektu a produkt **MEDIALOG** se nebude posouvat vpřed.

Bude-li pracovní zátěž pokračovat, bude váš neaktivní protokol bez omezení růst, protože nejstarší rozsah potřebný pro obnovu médií je stále potřebný a nelze jej znovu použít. Bude-li pracovní zátěž pokračovat, budete mít k dispozici systém souborů protokolu, který bude zcela zaplňován, aby problém vyřešil, než správce front začne odvolávat transakce a může dokonce náhle skončit.

Proto pro automatickou správu a správu protokolů archivace:

```
LogFilesystemSize > (PrimaryFiles + SecondaryFiles +
(((TimeBetweenMediaImages *2) + TimeNeededToResolveDamagedObject) * ExtentsUsedPerHour))
* LogFilePages
```

Poznámka: Předchozí algoritmus předpokládá, že **SET LOG ARCHIVED** je volán pro každou oblast, jakmile již není potřeba pro obnovu médií, pro správu archivního protokolu.

Správa protokolů

V produktu IBM MQ 9.1.0produkt podporuje automatickou správu protokolů a automatickou obnovu médií lineárních protokolů. Kruhové protokoly jsou téměř samoobslužné, ale někdy vyžadují zásah, aby se vyřešily problémy s prostorem.

Poznámka: IBM i Automatická správa a správa protokolů archivace nejsou v systému IBM iplatné.

Při kruhovém protokolování správce front uvolní prostor v souborech protokolu. Tato aktivita není uživateli zřejmá a obvykle se nezobrazuje velikost použitého místa na disku, protože přidělený prostor je rychle znovu využit.

V produktu IBM MQ 9.1.0 můžete odstranit sekundární soubory při použití kruhového protokolování. Další informace viz RESET QMGR **TYPE(REDUCELOG)** .

Při lineárním protokolování se protokol může zaplnit, pokud nebyl kontrolní bod již dlouhou dobu zabrán, nebo pokud dlouhotrvající transakce zapsala záznam protokolu před dlouhou dobou. Správce front se pokusí převzít kontrolní body dostatečně často, aby se vyhnul prvnímu problému.

Multi Pokud se protokol zaplní, vydá se zpráva AMQ7463 . Kromě toho, pokud se protokol zaplní, protože přerušitelná transakce zabránila uvolnění prostoru, vydá se zpráva AMQ7465 .

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.

V průběhu času se nejstarší zapsané záznamy protokolu stanou nepotřebnými pro restartování správce front.

Když je zjištěna přerušitelná transakce, je naplánována aktivita, která asynchronně odvolá tuto transakci. Pokud z nějakého neočekávaného důvodu došlo k selhání asynchronního odvolání, některá volání MQI v této situaci vrátí problém MQRC_RESOURCE_PROBLEM.

Všimněte si, že prostor je vyhrazen pro potvrzení nebo odvolání všech probíhajících transakcí, takže **MQCMIT** nebo **MQBACK** by nemělo selhat.

Aplikace, která má transakci odvolanou tímto způsobem, 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, je protokolovací prostor uvolněn a správce front pokračuje v normální činnosti.

Co se stane, když se disk zaplní

Je-li správce front konfigurován pro použití lineárního protokolování, komponenta protokolování správce front reaguje na stav zaplnění disku následujícími způsoby.

Pokud se disk obsahující soubory protokolu zaplní, pak:

- Správce front zjišťuje tuto podmínku pouze při vytváření nového souboru protokolu s požadovanou velikostí, který provádí před tím, než je potřeba.
- Zjistí stav zaplnění disku, když operační systém vrátí chybu z požadavku na rozšíření souboru na požadovanou velikost.
- Správce front vydá do protokolu chyb správce front zprávu AMQ6708 .
- Záznam FFST (First Failure Support Technology) je zapsán do adresáře chyb v rámci celého systému. Tento záznam poskytuje podrobnosti o stavu zaplnění disku a měl by být zachován, pokud potřebujete kontaktovat podporu IBM .

Soubory protokolu jsou vytvářeny v pevné velikosti, nikoli rozšiřovány, jak se do nich zapisují záznamy protokolu. To znamená, že produktu IBM MQ může dojít prostor na disku pouze tehdy, když vytváří nový soubor; nemůže dojít prostor, když zapisuje záznam do protokolu. Produkt IBM MQ vždy ví, kolik prostoru je k dispozici v existujících souborech protokolu, a spravuje prostor v souborech odpovídajícím způsobem.

Když v produktu IBM MQ 9.1.0použijete lineární protokolování, máte možnost použít:

- Automatická správa oblastí protokolu.

  Další informace o nových atributech protokolu viz DISPLAY QMSTATUS .

  Viz také následující příkazy nebo jejich ekvivalenty PCF:

  – RESET QMGR
  – SET LOG pro distribuované platformy
- Volby, které řídí použití obrazů médií.

  Další informace viz příkaz ALTER QMGR a příkaz ALTER QUEUES :

  – IMGINTVL
  – IMGLOGLN
  – IMGRCOVO
  – IMGRCOVQ
  – IMGSCHED

Kruhové protokolování vrací problém s prostředky.

Pokud vám stále dochází místo, zkontrolujte, zda je konfigurace protokolu v konfiguračním souboru správce front správná. Můžete být schopni snížit počet primárních nebo sekundárních souborů protokolu, aby protokol nezvýil dostupný prostor.

Velikost souborů protokolu pro existujícího správce front nelze změnit. Správce front vyžaduje, aby všechny oblasti protokolu byly stejné velikosti.

Správa souborů protokolu

Přidělte dostatek prostoru pro soubory protokolu. V případě lineárního protokolování můžete odstranit staré soubory protokolu, když již nejsou požadovány.

Informace specifické pro kruhové protokolování

Používáte-li kruhové protokolování, ujistěte se, že je při konfiguraci systému dostatek místa pro uložení souborů protokolu (viz “Sekce LogDefaults souboru mqs.ini” na stránce 93 a “Sekce protokolu souboru qm.ini” na stránce 130). Velikost prostoru na disku využitého protokolem se nezvýší nad konfigurovanou velikost, včetně prostoru pro sekundární soubory, které se mají vytvořit v případě potřeby.

Informace specifické pro lineární protokolování

Pokud používáte lineární protokol, soubory protokolu se přidávají průběžně, jak se protokolují data, a množství využitého místa na disku se s časem zvyšuje. Pokud je rychlost protokolovaných dat vysoká, prostor na disku je rychle využíván novými soubory protokolu.

V průběhu času již nejsou starší soubory protokolu pro lineární protokol nutné k restartování správce front nebo k provedení obnovy médií u poškozených objektů. Následující metody určují, které soubory protokolu jsou stále vyžadovány:

Zprávy událostí modulu protokolování
Dojde-li k významné události, například obrazu média záznamu, jsou generovány zprávy událostí modulu protokolování. Obsah zpráv událostí modulu protokolování určuje soubory protokolu, které jsou stále vyžadovány pro restartování správce front a zotavení z médií. Další informace o zprávách událostí modulu protokolování naleznete v tématu Události modulu protokolování .

Stav správce front
Spuštění příkazu MQSC, DISPLAY QMSTATUS nebo PCF, Inquire Queue Manager Status, vrátí informace o správci front včetně podrobností o požadovaných souborech protokolu. Další informace o příkazech MQSC naleznete v tématu Administrace IBM MQ pomocí příkazů MQSCa informace o příkazech PCF naleznete v tématu Automatizace administrativních úloh.

Zprávy správce front
Správce front pravidelně vydává dvojici zpráv, které označují, které soubory protokolu jsou potřebné:

- Zpráva AMQ7467I uvádí název nejstaršího souboru protokolu potřebného k restartování správce front. Tento soubor protokolu a všechny novější soubory protokolu musí být k dispozici během restartu správce front.
- Zpráva AMQ7468I uvádí název nejstaršího souboru protokolu potřebného pro obnovu médií.

Chcete-li určit "starší" a "novější" soubory protokolu, použijte číslo souboru protokolu, nikoli časy úprav použité systémem souborů.

Informace použitelné pro oba typy protokolování

Pouze soubory protokolu nezbytné pro restart správce front, aktivní soubory protokolu, musí být online. Neaktivní soubory protokolu lze zkopírovat na archivní médium, jako je páska pro zotavení z havárie, a odebrat je z adresáře protokolu. Neaktivní soubory protokolu, které nejsou vyžadovány pro obnovu médií, lze považovat za nadbytečné soubory protokolu. Nadbytečné soubory protokolu můžete odstranit, pokud již nejsou pro vaši operaci zajímavé.

Pokud nelze nalézt žádný potřebný soubor protokolu, je vydána zpráva operátora AMQ6767E . Zpřístupněte soubor protokolu a všechny následné soubory protokolu správci front a zopakujte operaci.

Automatické čištění oblastí protokolu-pouze lineární protokolování

Z produktu IBM MQ 9.1.0 máte možnost použít automatickou správu lineárních oblastí protokolu, které již nejsou pro obnovu vyžadovány.

Použijte atribut **LogManagement** v sekci Protokol souboru qm.ini nebo pomocí IBM MQ Explorer, abyste nastavili automatickou správu. Další informace viz “Sekce protokolu souboru qm.ini” na stránce 130.

Další podrobnosti o činnosti protokolu naleznete v parametru LOG v souboru **DISPLAY QMSTATUS** a v následujících příkazech pro použití protokolu:

- RESET QMGR
- Nastavit protokol

Automatické pořizování obrazů médií-pouze lineární protokolování

V produktu IBM MQ 9.1.0 existuje celkový přepínač pro řízení toho, zda správce front automaticky zapisuje obrazy médií, přičemž výchozí nastavení je, že přepínač nebyl nastaven.

Pomocí následujících atributů správce front můžete řídit, zda dojde k automatickému zobrazování médií, a frekvenci procesu:

IMGSCHED
Zda správce front zapisuje obrazy médií automaticky

IMGINTVL
Frekvence zápisu obrazů médií v minutách

IMGLOGLN
Megabajty protokolu zapsané od předchozího obrazu média objektu.

Máte-li kritický čas během dne, kdy je pracovní zátěž velmi vysoká, a chcete se ujistit, že propustnost systému není ovlivněna pořizováním automatických obrazů médií, můžete dočasně vypnout automatické zobrazování médií nastavením **IMGSCHED***(MANUAL)*.

Produkt **IMGSCHED** můžete kdykoli během pracovní zátěže přepnout.

Upozornění: MEDIALOG se neposouvá vpřed, pokud nepořizujete obrazy médií, takže musíte buď archivovat oblasti pro rozšíření, nebo se ujistěte, že máte dostatek místa na disku.

Můžete také řídit automatické a ruční obrazy médií pro jiné uživatelsky definované objekty pomocí atributu **IMGRCOVO** :

- Ověřovací informace
- Kanál
- Připojení klienta
- Modul listener
- Seznam názvů
- Proces
- Fronta aliasů
- Lokální fronta
- Služba
- Téma

Pro interní systémové objekty, například katalog objektů a objekt správce front, zapisuje správce front automaticky obrazy médií podle potřeby.

Další informace o atributech viz ALTER QMGR .

Můžete také povolit nebo zakázat automatické a ruční obrazy médií pouze pro lokální a trvalé dynamické fronty. To provedete pomocí atributu fronty **IMGRCOVQ** .

Další informace o atributu **IMGRCOVQ** viz ALTER QUEUES .

Notes:

1. Obrazy médií jsou podporovány pouze, pokud používáte lineární protokolování. Pokud jste povolili automatické obrazy médií, ale používáte kruhové protokolování, je vydána chybová zpráva a atribut automatických obrazů médií správce front je zakázán.
2. Pokud jste povolili automatické obrazy médií, ale neuvedli jste frekvenci, buď minuty, nebo megabajty protokolu, vydá se chybová zpráva a žádné automatické obrazy médií se nezapisují.

3. Obraz média můžete ručně zaznamenat pomocí příkazu rcdmqimg , pokud jste nastavili **IMGSCHED***(AUTO)*.

   To vám umožní pořizovat obrazy médií v době, která je vhodná pro váš podnik, například když je váš systém tichý. Automatické zobrazování médií bere v úvahu tyto manuální obrazy médií, protože ruční obraz média resetuje interval a délku záznamu, před kterým je pořízen další automatický obraz média.
4. V systému IBM MQ 9.1.0zapisuje správce front trvalé zprávy pouze v obrazech médií, nikoli v dočasných zprávách. To může snížit velikost obrazů médií při migraci na produkt IBM MQ 9.1.0 nebo novější

Rozhodování o tom, jak nastavit IMGLOGLN a IMGINTVL

V 9.3.4 Ve výchozím nastavení je parametr **IMGLOGLN** nastaven na hodnotu `off` pro správce front jiné než nativní správce front HA. (Nativní správci front HA jsou vytvářeni s hodnotou **IMGLOGLN** nastavenou na hodnotu 25% dostupného prostoru na svazku, do kterého mají být zapisovány protokoly pro zotavení.)

V 9.3.4 Standardně je parametr **IMGINTVL** nastaven na 60 minut. Interval určený parametrem **IMGINTVL** je uznán v případě, že ve správci front bylo provedeno dostatečné množství nové práce, aby bylo možné provést záznam nového obrazu. Jinak je pořizování nových obrázků zpožděno.

Můžete změnit hodnoty **IMGLOGLN** a **IMGINTVL** , abyste dosáhli nejlepšího řešení pro vaši konfiguraci. Nastavte **IMGLOGLN** a **IMGINTVL** dostatečně velké, aby správce front trávil pouze zlomek svého času zaznamenáváním obrazů médií, ale dostatečně malé, aby:

- Poškozené objekty mohou být obnoveny v přiměřené době a
- Dostatečně malý, aby se váš protokol vešel na disk bez nedostatku místa.

Nastavíte-li parametr **IMGLOGLN**, doporučuje se provést **IMGLOGLN** násobek množství dat ve frontách a mnohonásobek rychlosti přenosu dat pracovní zátěže. Čím větší je hodnota **IMGLOGLN**, tím méně času stráví správce front zaznamenáváním obrazů médií.

Podobně platí, že pokud nastavíte volbu **IMGINTVL**, doporučeným postupem je **IMGINTVL** tolikrát, kolik času správce front potřebuje k záznamu obrazu média. Můžete zjistit, jak dlouho trvá zaznamenat obraz média, tak, že jej zaznamenáte ručně.

Pokud jsou **IMGLOGLN** a **IMGINTVL** příliš velké, obnova poškozeného objektu může trvat velmi dlouho, protože všechny oblasti od posledního obrazu média musí být přehrány.

Nastavte hodnoty **IMGLOGLN** a **IMGINTVL** na dostatečně malé, aby byla pro vás přijatelná maximální doba potřebná k obnově poškozeného objektu.

Pokud jsou soubory **IMGLOGLN** a **IMGINTVL** velmi velké, znamená to, že protokol je velmi velký, protože obrazy médií jsou zaznamenávány tak zřídka.

Upozornění: Ujistěte se, že protokol této velikosti se pohodlně vejde do systému souborů protokolu, protože vaše pracovní zátěž bude vrácena zpět, pokud se systém souborů protokolu zcela zaplní.

Můžete nastavit jak **IMGINTVL** , tak **IMGLOGLN**. To může být užitečné, chcete-li zajistit, aby byly automatické obrazy médií pořízeny pravidelně během vysoké pracovní zátěže (řízené produktem **IMGLOGLN**), ale jsou stále pořízeny příležitostně, když je pracovní zátěž velmi lehká (řízená produktem **IMGINTVL**).

IMGINTVL a **IMGLOGLN** jsou cíle pro interval a délku dat protokolu, mezi kterými jsou pořizovány automatické obrazy médií.

Tyto atributy by neměly být považovány za pevné maximum nebo minimum. Ve skutečnosti se může správce front rozhodnout naplánovat automatický obraz média dříve, pokud správce front zjistí, že je opravdu dobrý čas:

- Vzhledem k tomu, že fronta je prázdná, je z hlediska výkonu nejefektivnější pořizování obrazu média a
- Obraz média nebyl po nějakou dobu zaznamenán

Příležitostně může být mezera mezi obrazy automatických médií o něco delší než **IMGINTVL** a **IMGLOGLN**.

Mezera mezi obrazy médií může být větší než **IMGLOGLN** , pokud se množství dat ve frontách blíží **IMGLOGLN**. Mezera mezi obrazy médií může být větší než **IMGINTVL** , pokud záznamu obrazu média trvá téměř stejně dlouho jako **IMGINTVL** .

Jedná se o špatný postup, protože správce front by trávil většinu času zaznamenáváním obrazů médií.

Při použití automatického záznamu obrazu média zaznamenává správce front obraz média pro každý objekt a frontu jednotlivě, takže správce front sleduje interval a délku protokolu mezi obrazy zvlášť pro každý objekt.

Postupně v průběhu času dochází k postupnému zaznamenávání mediálních obrazů, namísto záznamu mediálních obrazů pro všechny objekty současně. Tento ohromující rozprostírá dopad na výkon nahrávacích obrazů médií a je další výhodou použití automatického nahrávání obrazů médií oproti ručnímu nahrávání.

Ruční pořizování obrazů médií-pouze lineární protokolování

Záznam obrazu média fronty zahrnuje zápis všech trvalých zpráv z této fronty do protokolu. V případě front obsahujících velké objemy dat zpráv se jedná o zápis velkého množství dat do protokolu a tento proces může ovlivnit výkon systému v době, kdy k němu dochází.

Zaznamenávání obrazů médií jiných objektů bude pravděpodobně poměrně rychlé, protože obraz médií jiných objektů neobsahuje uživatelská data.

Je třeba pečlivě zvážit, kdy se mají zaznamenávat obrazy médií front, aby proces nekolidoval s vaší špičkovou pracovní zátěží.

Chcete-li aktualizovat nejstarší oblast protokolu potřebnou pro obnovu médií, musíte pravidelně zaznamenávat obraz média všech objektů.

Vhodný čas na záznam obrazu média fronty je, když je prázdný, protože v tomto okamžiku se do protokolu nezapisují žádná data zprávy. Naopak, špatný čas je, když je fronta velmi hluboká nebo má na sobě velmi velké zprávy.

Dobrý čas pro záznam obrazu média fronty je, když je váš systém tichý; zatímco špatný čas je během pracovní zátěže ve špičce. Pokud je vaše pracovní zátěž vždy o půlnoci tichá, můžete se například rozhodnout zaznamenávat obrazy médií každou noc o půlnoci.

Ohromující záznam každé z vašich front může rozšířit dopad na výkon, a tak snížit jeho účinek. Čím déle trvá od doby, kdy jste naposledy zaznamenali obrazy médií, tím důležitější je zaznamenávat je, protože počet oblastí protokolu požadovaných pro obnovu médií se zvyšuje.

Poznámka: Při provádění obnovy médií musí být všechny požadované soubory protokolu současně k dispozici v adresáři souborů protokolu. Ujistěte se, že máte pravidelné obrazy médií všech objektů, které chcete obnovit, abyste se vyhnuli nedostatku místa na disku, abyste zadrželi všechny požadované soubory protokolu.

Chcete-li například pořídit obraz média všech objektů ve správci front, spusťte příkaz **rcdmqimg** , jak je uvedeno v následujících příkladech:

Windows **zapWindows**

```
rcdmqimg -m QMNAME -t all *
```

Linux AIX **zapAIX and Linux**

```
rcdmqimg -m QMNAME -t all "*"
```

Spuštění příkazu **rcdmqimg** přesune pořadové číslo v protokolu médií (LSN) dopředu. Další podrobnosti o pořadových číslech protokolu viz “Výpis obsahu protokolu pomocí příkazu dmpmqlog” na stránce 646.

Produkt **rcdmqimg** se nespouští automaticky, proto musí být spuštěn ručně nebo z vámi vytvořené automatické úlohy. Další informace o tomto příkazu viz rcdmqimg a dmpmqlog.

Ruční záznam obrazů médií s produktem **rcdmqimg** pro správu protokolovacího prostoru není nutný, pokud jste zvolili použití lineárního protokolování s automatickým zobrazováním médií řízeným správcem front.

Poznámka: Zprávy AMQ7467 a AMQ7468 lze také zadat při spuštění příkazu `rcdmqimg` .

Dílčí obrazy médií

Je dobrým zvykem používat zprávy IBM MQ pouze pro data, u kterých se očekává, že budou v blízké budoucnosti spotřebována, takže každá zpráva bude ve frontě poměrně krátkou dobu.

Naopak je špatné používat zprávy IBM MQ k dlouhodobému ukládání dat jako databáze.

Je také dobrým zvykem zajistit, aby vaše fronty byly relativně mělké, a špatným postupem mít hluboké fronty, jejichž zprávy byly ve frontě po dlouhou dobu.

Podle těchto pokynů umožníte správci front optimalizovat výkon automatického záznamu obrazů médií.

Zaznamenávání obrazu média prázdné fronty je velmi efektivní (z hlediska výkonu), zatímco pořizování obrazu média fronty s velkým množstvím dat na ní je velmi neefektivní, protože všechna tato data musí být zapsána do protokolu v obrazu média.

Pro mělké fronty s nedávno vloženými zprávami může správce front provést další optimalizaci.

Pokud byly všechny zprávy, které jsou aktuálně ve frontě, vloženy do nedávné minulosti, může být správce front schopen zaznamenat obraz média jménem času (*bod zotavení*) těsně před vložením všech zpráv, a tak být schopen zaznamenat obraz prázdné fronty. Tento proces je velmi nízké náklady, pokud jde o výkon.

Pokud byly všechny zprávy, které byly ve frontě v bodu obnovy, následně přijaty, nemusí být tyto zprávy zaznamenány do obrazu média, protože již nejsou ve frontě.

Tomu se říká *částečný obraz média*. V nepravděpodobném případě, že je třeba obnovit frontu, budou přehrány všechny záznamy protokolů, které se vztahují k této frontě od posledního obrazu média, takže budou obnoveny všechny nedávno vložené zprávy.

I v případě, že ve frontě v bodě obnovy bylo několik zpráv, které jsou momentálně ve frontě (a proto musí být zaznamenány v částečném obrazu média), je stále efektivnější zaznamenat tento menší částečný obraz média, než úplný obraz média všech zpráv.

Zajištění toho, aby zprávy zůstaly ve frontách po krátkou dobu, pravděpodobně zlepší výkon automatického záznamu obrazů médií.

Určení nadbytečných souborů protokolu-pouze lineární protokolování
V případě kruhového protokolování nikdy neodstraňujte data z adresáře protokolu. Při správě lineárních souborů protokolu je důležité si být jisti, které soubory lze odstranit nebo archivovat. Tyto informace vám pomohou při rozhodování.

Nepoužívejte časy úprav systému souborů k určení "starších" souborů protokolu. Použijte pouze číslo souboru protokolu. Použití souborů protokolu správcem front se řídí složitými pravidly, včetně předběžného přidělení a formátování souborů protokolu před jejich potřebou. Můžete vidět soubory protokolu s časy úprav, které by byly zavádějící, pokud se pokusíte použít tyto časy k určení relativního stáří.

K určení nejstaršího potřebného souboru protokolu jsou k dispozici tři místa, která můžete použít:

- Příkaz DISPLAY QMSTATUS
- Zprávy událostí modulu protokolování a nakonec
- Zprávy protokolu chyb

Pro příkaz DISPLAY QMSTATUS se jedná o určení nejstaršího rozsahu protokolu potřebného pro:

- Restartujte správce front a zadejte příkaz `DISPLAY QMSTATUS RECLOG`.

- Proveďte obnovu médií, zadejte příkaz `DISPLAY QMSTATUS MEDIALOG`.
- Určete název pro oznámení o archivaci, zadejte příkaz `DISPLAY QMSTATUS ARCHLOG`.

Počet sekundárních oblastí protokolu při použití kruhového protokolování můžete snížit zadáním příkazu **RESET QMGR TYPE(REDUCELOG)**.

Obecně platí, že nižší číslo souboru protokolu znamená starší protokol. Pokud nemáte velmi vysoký obrat log souboru, v pořadí 3000 log souborů denně po dobu 10 let, nemusíte obstarávat číslo balení na 9 999 999 999. V tomto případě můžete archivovat libovolný soubor protokolu s číslem menším než hodnota RECLOG a můžete odstranit libovolný soubor protokolu s číslem menším než hodnoty RECLOG i MEDIALOG.

Upozornění: Soubor protokolu se zalomí, takže další číslo po 9 999 999 je nula.

Umístění souboru žurnálu
Při výběru umístění souborů protokolu nezapomeňte, že operace je vážně ovlivněna, pokud se produktu IBM MQ nepodaří naformátovat nový protokol kvůli nedostatku místa na disku.

Používáte-li cyklický protokol, ujistěte se, že je na jednotce dostatek prostoru pro alespoň konfigurované primární soubory protokolu. Ponechte také prostor pro alespoň jeden sekundární soubor protokolu, který je potřebný, pokud má protokol růst.

Používáte-li lineární protokol, uvolněte podstatně více prostoru; prostor spotřebovaný protokolem se při protokolování dat neustále zvětšuje.

Soubory protokolu byste měli umístit na oddělenou diskovou jednotku od dat správce front.

Integrita dat na tomto zařízení je prvořadá-měli byste povolit vestavěnou redundanci.

Také může být možné umístit soubory protokolu na více diskových jednotek v zrcadleném uspořádání. To chrání před selháním jednotky, která obsahuje protokol. Bez zrcadlení se můžete vrátit k poslední záloze systému IBM MQ .

Coldstart: Co dělat, když oblasti protokolu chybí nebo jsou poškozené

Pokud váš podnik ztratí některé nebo všechny oblasti protokolu potřebné pro zotavení při restartu, správce front nebude moci znovu přehrávat protokol pro zotavení, a proto se mu nepodaří jej restartovat. Pokud požadujete, aby se správce front restartoval, když je protokol pro zotavení jakýmkoli způsobem poškozen, na úkor zachování integrity dat, je to možné, i když je to velmi nevhodné. Tento proces je označován jako *studený start* správce front.

Důležité: Studený start správce front by měl být brán v úvahu pouze za výjimečných okolností a nese rizika integrity dat, jak je popsáno na této stránce. Produkt IBMnavrhuje, abyste v reakci na poškozené datové soubory znovu sestavili správce front namísto studeného spouštění.

Pokud je z provozních důvodů vyžadován studený start, obraťte se na zástupce podpory IBM a přezkoumejte základní příčinu problému. Při nejbližší příležitosti byste měli nahradit studeného spuštěného správce front znovu sestaveným správcem front.

Účinky studeného startu

Při studeném startu vytvoří správce front prázdný protokol pro zotavení a spoléhá se na data v souborech front a dalších souborech objektů v jejich existujícím stavu. Protože data v souborech fronty mohou být nekonzistentní, zprávy mohou být ztraceny, duplikovány, poškozeny nebo nekonzistentní.

Správce front ukládá konfiguraci všech ostatních trvalých objektů do protokolu pro zotavení i do souborů objektů. Do protokolu pro zotavení se také zaznamenávají další data vnitřního stavu, takže při studeném startu se vynulují data vnitřního stavu a všechna tato další konfigurační data mohou být nepřesná.

Účinky studeného startu jsou nepředvídatelné a rozsáhlé, takže byste se měli vyvarovat studeného startu, pokud to není nezbytně nutné. Po studeném spuštění mohou být informace ve frontě a v objektových souborech tak nekonzistentní, že správce front nebude vůbec restartován.

Pokud se správce front restartuje, neexistuje jednoduchý způsob, jak zjistit, na která data zprávy nebo konfiguraci lze spoléhat a co ne. Také po studeném startu mohou být fronty poškozeny, a tak se stávají zcela nepoužitelnými.

Navíc, pokud můžete získat nebo vložit do určité fronty, mohou být zprávy na ní poškozené, chybějící nebo duplicitní. Transakce a kanály mohou být uváznuté v nejistém stavu. I když se váš správce front úspěšně spustí a fronty budou vypadat neporušené, nepředvídatelné účinky studeného startu nemusí být realizovány až mnohem později.

Co dělat, když potřebujete studenstart

Provedení studeného startu by nemělo být považováno za standardní provozní praxi a IBM vás od toho silně odrazuje. Pokud se však nacházíte v pozici, kde je rozhodně nutné správce front studenovat, obraťte se na adresu IBM MQ Podpora .

Proces studenového spouštění správce front byl pro liniového správce front mnohem komplikovanější než cyklický. V produktu IBM MQ 9.1.3byl proces studeného startu výrazně zjednodušen a nezahrnuje již kopírování ani přejmenování oblastí protokolu.

V operačním systému IBM MQ 9.1.3se obraťte na podporu společnosti IBM , která vám poskytne klíč, který předáte příkazu **strmqm** ke studenému spuštění správce front.

Upozornění: Příkaz IBM MQ 9.1.3 coldstart stále nese stejná rizika ztráty integrity dat jako ruční studený start a IBM vás od toho silně odrazuje.

Eliminace budoucích studených spuštění: požadavek

Příkaz strmqm vyžaduje klíč pro studený start, protože IBM MQ chce, abyste kontaktovali podporu IBM MQ , pokud potřebujete studený start, protože IBM MQ má zájem pochopit, jak jste se dostali do této situace.

Je zřejmé, že chladný start je něco, co se nejlépe vyhnout. Produkt IBM MQ vynaložil značné úsilí na to, abyste se ujistili, že nebudete muset studenatovat spuštění správce front, a produkt IBM se snaží zjistit, zda existuje něco víc, co může produkt udělat pro zmírnění nutnosti studenéhostartu.

Opatření, která se mají vyhnout studený start

Výchozí metodou protokolování při vytváření správce front je kruhové protokolování. S kruhovým protokolováním povolíte správci front určitý počet primárních a sekundárních oblastí protokolu dané velikosti. Vytvořte systém souborů protokolu dostatečně velký na to, aby obsahoval všechny primární a sekundární oblasti protokolu, a nikdy byste je neměli spravovat.

Alternativně můžete použít lineární protokolování na rozdíl od kruhového. Lineární protokolování vám dává přidanou schopnost obnovit fronty a další objekty, v nepravděpodobném případě, že se poškodí. Při výchozím nastavení však lineární protokolování vyžaduje, abyste odstranili oblasti protokolu, které již nejsou potřebné pro restart nebo obnovu médií. Na tuto správu se odkazuje jako na ruční správu protokolů.

Při správě oblastí protokolu tímto způsobem je možné neúmyslně odstranit příliš mnoho oblastí protokolu, a tak skončit s chladným startem. Chcete-li toto riziko zmírnit, použijte automatickou správu protokolů, aby správce front spravoval oblasti protokolu vaším jménem.

Doporučeným postupem je umístit protokol pro zotavení do samostatného systému souborů protokolu, který obsahuje pouze protokol pro zotavení. Pokud vložíte protokol pro zotavení do stejného systému souborů jako zbytek správce front, můžete někdy zjistit, že se systém souborů náhodně zaplňuje, například kvůli velkým souborům ve frontě. Buď nastavte adresář protokolu pro správce front jako samostatný systém souborů, nebo zadejte jiný systém souborů protokolu pomocí volby příkazového řádku **-ld** v příkazu **crtmqm** .

Pokud se souborový systém, který zadržuje soubory fronty, zaplní, možná nebudete moci do těchto front vkládat, ale správce front bude pokračovat. Pokud se souborový systém obsahující protokol pro zotavení zaplní, správce front se náhle ukončí a nebude restartován, dokud neuvolníte místo.

Dávejte pozor, abyste neodstranili oblasti protokolu potřebné pro obnovu po restartu, jinak byste se mohli ocitnout v situaci, že byste museli provést studendstart. Někdy zjistíte, že je třeba provést studený start, protože došlo k selhání disku, který obsahuje jejich protokol pro zotavení. Doporučeným postupem je umístit protokol pro zotavení na replikovaný disk, a snížit tak riziko havárie disku.

Přesunutím zpráv a konfigurace do nového náhradního správce front se vyhnete možným problémům s dříve studeným spuštěním správce front.

Poznamenejte si, kteří správci front byli dříve studeni, a to i v případě, že byli studenově spuštěni před dlouhou dobou a mezitím byli zastaveni, restartováni a migrováni. Když se obrátíte na podporu IBM , řekněme, že správce front byl dříve studený start, a pokud ano, poskytněte co nejvíce informací o tom, co způsobilo požadavek na studený start.

Použití protokolu pro zotavení

Můžete použít informace z protokolů, které vám pomohou zotavit se ze selhání.

Existuje několik způsobů, jak mohou být vaše data poškozena. IBM MQ vám pomůže zotavit se z:

- Poškozený datový objekt
- Ztráta napájení v systému
- Selhání komunikace

Tento oddíl se zabývá tím, jak se protokoly používají k zotavení z těchto problémů.

Obnova po výpadku napájení nebo selhání komunikace

Produkt IBM MQ se může zotavit ze selhání komunikace i ze ztráty napájení. Může se také někdy zotavit z jiných typů problémů, jako je neúmyslné odstranění souboru.

V případě selhání komunikace zůstávají trvalé zprávy ve frontách, dokud nejsou odebrány přijímající aplikací. Pokud je zpráva přenášena, zůstává v přenosové frontě, dokud ji nelze úspěšně přenést. Chcete-li se zotavit ze selhání komunikace, můžete obvykle restartovat kanály pomocí linky, která selhala.

Dojde-li ke ztrátě napájení, při restartování správce front IBM MQ obnoví v době selhání fronty do jejich potvrzeného stavu. Tím se zajistí, že nebudou ztraceny žádné trvalé zprávy. Dočasné zprávy jsou vyřazeny; nepřežijí, když se produkt IBM MQ náhle zastaví.

Obnova poškozených objektů

Existují způsoby, jak se objekt IBM MQ může stát nepoužitelným, například kvůli neúmyslnému poškození. Pak musíte obnovit buď celý systém, nebo jeho část. Požadovaná akce závisí na tom, kdy je zjištěno poškození, na tom, zda vybraná metoda protokolu podporuje obnovu médií a které objekty jsou poškozené.

Náprava média

Můžete zaznamenávat obrazy médií pro objekty, aby mohly být obnoveny, pokud jsou poškozeny. Tato funkce je k dispozici pouze pro správce front, kteří používají lineární protokolování nebo replikované protokolování , a pro lineární protokolování pouze pro objekty, které jsou definovány jako obnovitelné. Typy objektů lze obnovit pomocí atributů správce front **IMGRCOVO** a **IMGRCOVQ** . Viz ALTER QMGR. Pokud je objekt, který není definován jako obnovitelný, poškozen, pak volby obnovy jsou stejné jako pro kruhové protokolování.

Obnova médií znovu vytvoří objekty z informací zaznamenaných v lineárním protokolu nebo replikovaném protokolu. Pokud je například soubor objektu neúmyslně odstraněn nebo se stane nepoužitelným z jiného důvodu, může jej obnova médií znovu vytvořit. Informace v protokolu požadované pro obnovu médií objektu se nazývají *obraz média*.

Obraz média je posloupnost záznamů protokolu obsahující obraz objektu, ze kterého lze znovu vytvořit samotný objekt.

První záznam protokolu požadovaný k opětovnému vytvoření objektu je znám jako jeho *záznam obnovy médií*; jedná se o začátek nejnovějšího obrazu média pro objekt. Záznam obnovy médií každého objektu je jednou z informací zaznamenaných během kontrolního bodu.

Když je objekt znovu vytvořen ze svého obrazu média, je také nutné přehrát všechny záznamy protokolu popisující aktualizace provedené na objektu od posledního pořízeného obrazu.

Zvažte například lokální frontu, která má obraz objektu fronty pořízený před vložením trvalé zprávy do fronty. Aby bylo možné znovu vytvořit nejnovější obraz objektu, je nutné přehrát záznamy protokolu, které zaznamenávají vložení zprávy do fronty, kromě přehrání samotného obrazu.

Když je vytvořen objekt, zapsané záznamy protokolu obsahují dostatek informací pro úplné opětovné vytvoření objektu. Tyto záznamy tvoří první obraz média objektu. Při každém ukončení pak správce front zaznamenává obrazy médií automaticky následujícím způsobem:

- Obrazy všech objektů procesu a front, které nejsou lokální
- Obrazy prázdných lokálních front

Obrazy médií lze zaznamenávat také ručně pomocí příkazu **rcdmqimg** , který je popsán v části rcdmqimg. Tento příkaz zapíše obraz média objektu IBM MQ .

Správce front zaznamenává obrazy médií automaticky, je-li nastavena hodnota **IMGSCHED***(AUTO)* . Další informace viz ALTER QMGR , kde naleznete informace o **IMGINTVL** a **INGLOGLN**.

Po zápisu obrazu média jsou k opětovnému vytvoření poškozených objektů vyžadovány pouze protokoly, které uchovávají obraz média, a všechny protokoly vytvořené po této době. Přínos vytváření obrazů médií závisí na takových faktorech, jako je množství dostupného volného úložiště a rychlost vytváření souborů protokolu.

Obnova z obrazů médií

Správce front automaticky obnoví některé objekty z obrazu média během spuštění správce front. Obnoví frontu automaticky, pokud byla zahrnuta do jakékoli transakce, která byla neúplná, když byl správce front naposledy ukončen, a bylo zjištěno, že je poškozena nebo poškozena během zpracování restartu.

Ostatní objekty musíte obnovit ručně pomocí příkazu **rcrmqobj** , který přehraje záznamy v protokolu a znovu vytvoří objekt IBM MQ . Objekt je znovu vytvořen z nejnovějšího obrazu nalezeného v protokolu spolu se všemi použitelnými událostmi protokolu mezi okamžikem uložení obrazu a okamžikem zadání příkazu opětovného vytvoření. Pokud dojde k poškození objektu IBM MQ , jediné platné akce, které lze provést, jsou buď jeho odstranění, nebo jeho opětovné vytvoření touto metodou. Přechodné zprávy nelze tímto způsobem obnovit.

Další podrobnosti o příkazu **rcrmqobj** viz rcrmqobj .

Soubor protokolu obsahující záznam o zotavení média a všechny následné soubory protokolu musí být k dispozici v adresáři souboru protokolu při pokusu o zotavení objektu z média. Pokud požadovaný soubor nelze nalézt, je vydána zpráva operátora AMQ6767 a operace obnovy média selže. Pokud nepoužíváte pravidelné obrazy médií objektů, které chcete znovu vytvořit, můžete mít nedostatek místa na disku, abyste zadrželi všechny soubory protokolu potřebné k opětovnému vytvoření objektu.

V 9.3.3 Nativní správci front HA používají replikované protokolování. Tito správci front se při zjištění poškození pokusí o automatické zotavení vhodných objektů. Po spuštění se nativní správci front vysoké dostupnosti standardně automaticky pokusí o asynchronní zotavení při zjištění poškození objektu. Obnova nemusí být okamžitě možná, pokud je například objekt používán aplikací, nebo pokud nejsou k dispozici oblasti protokolu požadované pro obnovu médií. V těchto situacích se asynchronní zpracování obnovy pravidelně opakuje. Pokud je problém, který zabránil obnově, vyřešen, objekt bude obnoven při dalším pokusu, nebo jej lze obnovit ručně pomocí příkazu **rcrmqobj** .

Jaké soubory objektů existují

Správce front ukládá atributy objektů, které jsou definovány v souboru **runmqsc** , do souborů na disku. Tyto soubory objektů se nacházejí v podadresářích pod datovým adresářem správce front.

Linux AIX Například na platformách AIX and Linux jsou kanály uloženy v adresáři `/var/mqm/qmgrs/qmgr/channel`.

Data v těchto souborech objektů jsou mediální obraz objektů. Pokud jsou tyto soubory objektů odstraněny nebo poškozeny, objekt uložený v tomto souboru je poškozen. Pomocí správce front lineárního protokolování lze poškozené objekty obnovit z protokolu pomocí příkazu rcrmqobj . Při zjištění poškozených objektů se správci front s replikovaným protokolováním (Native HA) automaticky pokusí o zotavení poškozených objektů.

Většina souborů objektů obsahuje pouze atributy objektu, takže soubory kanálů obsahují atributy kanálů. Výjimky jsou:

- Katalog

  Katalog objektů katalogizuje všechny objekty všech typů a je uložen v adresáři `qmanager/QMQMOBJCAT`.
- Synchronizovat soubory

  Synchronizační soubor obsahuje interní stavové údaje přidružené ke všem kanálům.
- Fronty

  Soubory fronty obsahují jak zprávy v této frontě, tak i atributy této fronty.

Všimněte si, že v produktu **runmqsc** nebo IBM MQ Explorernení vystaven žádný katalog nebo objekt syncfile.

Katalog a správce front lze zaznamenat, ale nelze je obnovit. Pokud dojde k poškození těchto objektů, správce front se ukončí preventivně a tyto objekty se při restartu automaticky obnoví.

Odběry nejsou uvedeny v objektech, které mají být zaznamenány nebo obnoveny, protože trvalé odběry jsou uloženy v systémové frontě. Chcete-li zaznamenat nebo obnovit trvalé odběry, zaznamenejte nebo obnovte systém SYSTEM.DURABLE.SUBSCRIBER.QUEUE místo toho.

Obnova poškozených objektů během spuštění

Pokud správce front zjistí při spuštění poškozený objekt, akce, kterou provede, závisí na typu objektu a na tom, zda je správce front konfigurován tak, aby podporoval obnovu médií.

Je-li objekt správce front poškozen, nelze jej spustit, pokud není schopen objekt obnovit. Pokud je správce front konfigurován s lineárním protokolem, a proto podporuje obnovu médií, produkt IBM MQ se automaticky pokusí znovu vytvořit objekt správce front z jeho obrazů médií. Pokud vybraná metoda protokolování nepodporuje zotavení z médií, můžete buď obnovit zálohu správce front, nebo odstranit správce front.

Pokud byly při zastavení správce front aktivní nějaké transakce, jsou k úspěšnému spuštění správce front vyžadovány také lokální fronty obsahující trvalé, nepotvrzené zprávy vložené nebo přijaté uvnitř těchto transakcí. Pokud je některá z těchto lokálních front poškozena a správce front podporuje obnovu médií, automaticky se je pokusí znovu vytvořit z jejich obrazů médií. Nelze-li některou z front obnovit, IBM MQ nelze spustit.

Pokud jsou během zpracování spuštění ve správci front, který nepodporuje zotavení z médií, zjištěny poškozené lokální fronty obsahující nepotvrzené zprávy, budou tyto fronty označeny jako poškozené objekty a nepotvrzené zprávy v nich budou ignorovány. Tato situace je způsobena tím, že není možné provést obnovu médií poškozených objektů v takovém správci front a jedinou zbývající akcí je jejich odstranění. Je vydána zpráva AMQ7472 pro ohlášení jakéhokoli poškození.

Obnova poškozených objektů jindy

Obnova médií objektů je automatická pouze během spuštění (jiné než pro nativní správce front HA, kteří standardně používají automatické zotavení). Jindy, když je zjištěno poškození objektu, je vydána zpráva operátora AMQ7472 a většina operací používajících objekt selže s návratovým kódem MQRC_OBJECT_DAMAGE. Dojde-li k poškození objektu správce front kdykoli po spuštění správce front, provede správce front preventivní ukončení. Pokud byl objekt poškozen, můžete jej odstranit, nebo pokud

správce front používá lineární protokol, pokuste se jej obnovit z obrazu média pomocí příkazu **rcrmqobj** (další podrobnosti viz rcrmqobj).

Pokud dojde k poškození fronty (nebo jiného objektu), produkt **MEDIALOG** se neposune vpřed. Důvodem je, že **MEDIALOG** je nejstarší oblast vyžadovaná pro obnovu médií. Pokud vaše pracovní zátěž pokračuje, produkt **CURRLOG** bude i nadále pokračovat, a proto budou zapsány nové oblasti. V závislosti na konfiguraci (včetně nastavení **LogManagement**) může dojít k zaplnění systému souborů protokolu. Pokud se systém souborů protokolu úplně zaplní, transakce se odvolá a správce front může náhle skončit. Dojde-li tedy k poškození fronty, je možné, že před ukončením správce front budete mít k dispozici pouze omezené množství času. Doba, kterou máte, závisí na rychlosti, jakou vaše pracovní zátěž způsobuje, že správce front zapisuje nové oblasti, a na množství volného místa, které máte v systému souborů protokolu.

Používáte-li ruční správu protokolů, může se stát, že archivujete oblasti, které nejsou potřebné pro obnovu po restartu, a pak je odstraníte ze systému souborů protokolu, i když jsou stále potřebné pro obnovu médií. To je přijatelné, pokud je můžete v případě potřeby obnovit z archivu. Tato zásada nezpůsobí, že se systém souborů protokolu zaplní, když dojde k poškození fronty a produkt **MEDIALOG** přestane postupovat vpřed. Pokud však archivujete a odstraňujete pouze oblasti, které nejsou potřebné pro restart ani pro obnovu médií, systém souborů protokolu se začne zaplňovat, pokud dojde k poškození fronty.

Pokud používáte automatickou správu protokolu nebo správu protokolu archivu, nebude správce front opakovaně používat oblasti, které jsou stále potřebné pro zotavení z médií, i když jste je možná archivovali a upozornili správce front pomocí příkazu SET LOG ARCHXX_ENCODE_CASE_ONE website. V důsledku toho, pokud dojde k poškození fronty, začne se zaplňovat systém souborů protokolu.

Dojde-li k poškození fronty, budou zapsány záznamy FFDC OBJECT POŠKOZENÉ a systém **MEDIALOG** přestane pokračovat. Poškozený objekt lze identifikovat z komponenty FFDC nebo proto, že se jedná o objekt s nejstarším objektem **MEDIALOG** při zobrazení jeho stavu v souboru **runmqsc**.

Pokud se váš systém souborů protokolu zaplňuje a máte obavy, že se vaše pracovní zátěž odvolává, protože se systém souborů protokolu zaplňuje, pak obnovení objektu nebo uvedení pracovní zátěže do klidového stavu může tuto situaci zastavit.

V 9.3.3 V případě nativních správců front HA (kteří používají replikované protokolování) je proveden pokus o automatické zotavení poškozených objektů. Po spuštění se nativní správci front vysoké dostupnosti standardně automaticky pokusí o asynchronní zotavení při zjištění poškození objektu. Obnova nemusí být okamžitě možná, pokud je například objekt používán aplikací, nebo pokud nejsou k dispozici oblasti protokolu požadované pro obnovu médií. V těchto situacích se asynchronní zpracování obnovy pravidelně opakuje. Pokud je problém, který zabránil obnově, vyřešen, objekt bude obnoven při dalším pokusu, nebo jej lze obnovit ručně pomocí příkazu **rcrmqobj** .

Ochrana souborů protokolu IBM MQ

Nedotkněte se souborů protokolu, když je spuštěn správce front, zotavení může být nemožné. K ochraně souborů protokolu před neúmyslnými úpravami použijte oprávnění superuživatele nebo mqm.

Neodebírejte soubory aktivního protokolu ručně, když je spuštěn správce front IBM MQ . Pokud uživatel neúmyslně odstraní soubory protokolu, které správce front potřebuje restartovat, produkt IBM MQ **nevydá** žádné chyby a pokračuje ve zpracování dat *včetně trvalých zpráv*. Správce front se vypíná normálně, ale jeho restartování se může nezdařit. Obnova zpráv se pak stává nemožnou.

Uživatelé s oprávněním k odebírání protokolů používaných aktivním správcem front mají také oprávnění k odstraňování dalších důležitých prostředků správce front (například souborů front, katalogu objektů a spustitelných souborů IBM MQ). Mohou proto poškodit spuštěného nebo neaktivního správce front, například nezkušením, způsobem, před kterým se produkt IBM MQ nemůže chránit.

Při udělování oprávnění superuživatele nebo mqm postupujte opatrně.

Výpis obsahu protokolu pomocí příkazu dmpmqlog

Jak použít příkaz dmpmqlog k výpisu obsahu protokolu správce front.

Pomocí příkazu dmpmqlog můžete vypsat obsah protokolu správce front. Standardně se vypisují všechny aktivní záznamy protokolu, to znamená, že příkaz začne vypisovat výpis z hlavičky protokolu (obvykle začátek posledního dokončeného kontrolního bodu).

Protokol lze obvykle vypsat pouze v případě, že není spuštěn správce front. Vzhledem k tomu, že správce front provádí kontrolní bod během ukončování práce systému, aktivní část protokolu obvykle obsahuje malý počet záznamů protokolu. Pomocí příkazu dmpmqlog však můžete vypsat více záznamů protokolu pomocí jedné z následujících voleb pro změnu počáteční pozice výpisu:

- Spusťte výpis paměti ze *základu* protokolu. Základem protokolu je první záznam protokolu v souboru protokolu, který obsahuje hlavičku protokolu. Množství dalších dat vypsaných v tomto případě závisí na tom, kde je hlavička protokolu umístěna v souboru protokolu. Pokud je blízko začátku souboru protokolu, vypíše se pouze malé množství dalších dat. Pokud se hlavička nachází na konci souboru protokolu, vypíše se výrazně více dat.
- Zadejte počáteční pozici výpisu paměti jako individuální záznam protokolu. Každý záznam protokolu je identifikován jedinečným *pořadovým číslem protokolu (LSN)*. V případě kruhového protokolování nemůže být tento počáteční záznam protokolu před základem protokolu; toto omezení se nevztahuje na lineární protokoly. Možná budete muset před spuštěním příkazu obnovit neaktivní soubory protokolu. Jako počáteční pozici je třeba určit platné číslo LSN převzaté z předchozího výstupu příkazu dmpmqlog .

  Například s lineárním protokolováním můžete zadat nextlsn z posledního výstupu příkazu dmpmqlog . nextlsn se objeví v souboru Log File Header a označuje LSN dalšího záznamu protokolu, který se má zapsat. Toto použijte jako počáteční pozici pro formátování všech záznamů protokolu zapsaných od posledního výpisu protokolu.
- **Pouze pro lineární protokoly**můžete instruovat dmpmqlog , aby začal formátovat záznamy protokolu z libovolného rozsahu daného souboru protokolu. V tomto případě příkaz dmpmqlog očekává, že tento soubor protokolu a každý po sobě jdoucí soubor protokolu nalezne ve stejném adresáři jako soubory aktivního protokolu. Tato volba se nevztahuje na kruhové protokoly, kde dmpmqlog nemá přístup k záznamům protokolu před základem protokolu.

Výstup příkazu dmpmqlog je Log File Header a řada formátovaných záznamů protokolu. Správce front používá několik záznamů protokolu k zaznamenávání změn svých dat.

Některé z formátovaných informací se používají pouze interně. Následující seznam obsahuje nejužitečnější záznamy protokolu:

Hlavička souboru žurnálu.
Každý protokol má jedno záhlaví souboru protokolu, což je vždy první věc naformátovaná příkazem dmpmqlog . Obsahuje následující pole:

logactive	Počet primárních oblastí protokolu.
loginactive	Počet sekundárních oblastí protokolu.
logsize	Počet stránek o velikosti 4 kB na oblast pro rozšíření.
baselsn	První LSN v oblasti protokolu obsahující záhlaví protokolu.
nextlsn	Číslo LSN dalšího záznamu protokolu, který má být zapsán.
headlsn	Číslo LSN záznamu protokolu v záhlaví protokolu.
tailsn	Číslo LSN identifikující zadní pozici protokolu.
hflag1	Zda je protokol CIRCULAR nebo LOG RETAIN (lineární).
HeadExtent	Oblast protokolu obsahující záhlaví protokolu.

Záhlaví záznamu protokolu
Každý záznam protokolu v protokolu má pevné záhlaví obsahující následující informace:

LSN	Pořadové číslo v protokolu.
LogRecd	Typ záznamu protokolu.

XTranid	Identifikátor transakce přidružený k tomuto záznamu protokolu (pokud existuje). *TranType* MQI označuje transakci typu IBM MQonly. Produkt *TranType* s podporou XA je zapojen do jiných správců prostředků. Aktualizace zahrnuté v rámci stejné pracovní jednotky mají stejnou hodnotu *XTranid*.
QueueName	Fronta přidružená k tomuto záznamu protokolu (pokud existuje).
Qid	Jedinečný interní identifikátor pro frontu.
PrevLSN	Číslo LSN předchozího záznamu protokolu v rámci stejné transakce (pokud existuje).

Spustit správce front
Tímto se protokoluje, že byl spuštěn správce front.

StartDate	Datum, kdy byl spuštěn správce front.
StartTime	Čas spuštění správce front.

Zastavit správce front
Tímto se protokoluje, že správce front byl zastaven.

StopDate	Datum, kdy byl správce front zastaven.
StopTime	Čas, kdy byl správce front zastaven.
ForceFlag	Typ použitého ukončení práce systému.

Počáteční kontrolní bod
To označuje spuštění kontrolního bodu správce front.

Koncový kontrolní bod
To označuje konec kontrolního bodu správce front.

ChkPtChkPt	Číslo LSN záznamu protokolu, který spustil tento kontrolní bod.

Vložit zprávu
Tímto se protokoluje trvalá zpráva vložená do fronty. Pokud byla zpráva vložena do synchronizačního bodu, záhlaví záznamu protokolu obsahuje nenulovou hodnotu *XTranid*. Zbytek záznamu obsahuje:

MapIndex	Identifikátor pro zprávu ve frontě. Lze jej použít pro shodu s odpovídajícím příkazem MQGET , který byl použit k získání této zprávy z fronty. V tomto případě lze nalézt následný záznam protokolu *Get Message* obsahující stejné položky QueueName a MapIndex. V tomto bodě lze identifikátor MapIndex znovu použít pro následnou vloženou zprávu do této fronty.
Data	Výpis paměti hex pro tento záznam protokolu obsahuje různá interní data, následovaná reprezentací deskriptoru zprávy (eyecatcher MD) a poté samotná data zprávy.

Vložit část
Trvalé zprávy, které jsou příliš velké pro jeden záznam protokolu, jsou protokolovány jako více záznamů protokolu *Put Part* následovaných jedním záznamem *Put Message* . Pokud existují záznamy *Put Part* , pak pole *PrevLSN* zřetězuje záznamy *Put Part* a konečný záznam *Put Message* dohromady.

Data	Pokračuje v datech zprávy, kde byl předchozí záznam protokolu vypnut.

Získat zprávu
Protokolují se pouze trvalé zprávy. Pokud byla zpráva získána pod synchronizačním bodem, záhlaví záznamu protokolu obsahuje nenulovou hodnotu *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, která je pouze IBM MQ. TranType XA označuje typ, který zahrnuje jiné správce prostředků. Všechny aktualizace provedené touto transakcí budou mít stejnou hodnotu *XTranid*.

Připravit transakci
Označuje, že je správce front připraven potvrdit aktualizace přidružené k zadanému souboru *XTranid*. Tento záznam protokolu je zapsán jako součást dvoufázového potvrzování zahrnujícího další správce prostředků.

Potvrdit transakci
Označuje, že správce front provedl všechny aktualizace provedené transakcí.

Odvolat transakci
To označuje záměr správce front odvolat transakci.

Ukončení transakce
To označuje konec odvolané transakce.

Tabulka transakcí
Tento záznam je zapsán během synchronizačního bodu. Zaznamenává stav každé transakce, která provedla trvalé aktualizace. Pro každou transakci se zaznamenávají tyto informace:

XTranid	Identifikátor transakce.
FirstLSN	Číslo LSN prvního záznamu protokolu přidruženého k transakci.
LastLSN	Číslo LSN posledního záznamu protokolu přidruženého k transakci.

Účastníci transakce
Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Zaznamenává externí správce prostředků, kteří se účastní transakcí. Pro každého účastníka se zaznamenávají tyto údaje:

Název RMName	Název správce prostředků.
RMID	Identifikátor správce prostředků. To je také zaprotokolováno v následných záznamech protokolu *Transaction Prepared* , které zaznamenávají globální transakce, jichž se správce prostředků účastní.
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 uvedená globální transakce byla úspěšně připravena. Každý ze zúčastněných správců prostředků bude instruován k potvrzení. Soubor *RMID* každého připraveného správce prostředků je zaznamenán v záznamu protokolu. Pokud se samotný správce front účastní transakce, bude přítomna hodnota *Participant Entry* s hodnotou *RMID* nula.

Zapomenout na transakci
Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Sleduje záznam protokolu *Transaction Prepared* , když bylo rozhodnutí o potvrzení doručeno každému účastníkovi.

Vyprázdnit frontu
Do protokolu je zaznamenáno, že všechny zprávy ve frontě byly vyprázdněny, například pomocí příkazu MQSC CLEAR QUEUE.

Atributy fronty
Tím se protokoluje inicializace nebo změna atributů fronty.

Vytvořit objekt
Tím se protokoluje vytvoření objektu IBM MQ .

ObjName	Název objektu, který byl vytvořen.
UserId	ID uživatele, který provádí vytvoření.

Odstranit objekt
Tím se protokoluje odstranění objektu IBM MQ .

ObjName	Název objektu, který byl odstraněn.

Zálohování a obnova dat správce front IBM MQ

Správce front můžete chránit před možným poškozením způsobeným selháním hardwaru zálohováním správců front a dat správců front, zálohováním pouze konfigurace správce front a použitím záložního správce front.

Informace o této úloze

POZOR: Pokud přesunete správce front do jiného operačního systému, musíte být velmi opatrní. Další informace naleznete v tématu Přesunutí správce front do jiného operačního systému .

Pravidelně můžete provádět opatření na ochranu správců front před možným poškozením způsobeným selháním hardwaru. Existují tři způsoby ochrany správce front:

Zálohovat data správce front
Dojde-li k selhání hardwaru, může být vynuceno zastavení správce front. Dojde-li ke ztrátě dat protokolu správce front v důsledku selhání hardwaru, je možné, že správce front nebude možné restartovat. Pokud zálohujete data správce front, můžete obnovit některá nebo všechna ztracená data správce front.

Obecně platí, že čím častěji zálohujete data správce front, tím méně dat ztratíte v případě selhání hardwaru, což má za následek ztrátu integrity protokolu zotavení.

Chcete-li zálohovat data správce front, nesmí být spuštěn správce front.

Zálohovat pouze konfiguraci správce front
Dojde-li k selhání hardwaru, může být vynuceno zastavení správce front. Pokud dojde v důsledku selhání hardwaru ke ztrátě konfigurace správce front i dat protokolu, nelze správce front restartovat nebo obnovit z protokolu. Pokud zálohujete konfiguraci správce front, můžete znovu vytvořit správce front a všechny jeho objekty z uložených definic.

Chcete-li zálohovat konfiguraci správce front, musí být spuštěn správce front.

Použít záložního správce front
Pokud je selhání hardwaru závažné, může být správce front neobnovitelný. V této situaci platí, že pokud má neobnovitelný správce front vyhrazeného záložního správce front, lze tohoto záložního správce front aktivovat namísto neobnovitelného správce front. Je-li protokol pravidelně aktualizován, může záložní protokol správce front obsahovat data protokolu, která obsahují poslední úplný protokol ze správce front, který nelze obnovit.

Záložního správce front lze aktualizovat v době, kdy je stávající správce front stále spuštěn.

Procedura

- Chcete-li zálohovat a obnovit data správce front, postupujte takto:
  - “Zálohování dat správce front” na stránce 651.
  - “Obnovení dat správce front” na stránce 652.
- Chcete-li zálohovat a obnovit konfiguraci správce front, postupujte takto:
  - “Zálohování konfigurace správce front” na stránce 652
  - “Obnovení konfigurace správce front” na stránce 653
- Chcete-li vytvořit, aktualizovat a spustit záložního správce front, postupujte podle části “Použití záložního správce front” na stránce 654.

Zálohování dat správce front

Zálohování dat správce front vám může pomoci chránit před možnou ztrátou dat způsobenou hardwarovými chybami.

Než začnete

Před spuštěním zálohování správce front se ujistěte, že správce front není spuštěn. Pokud se pokusíte vytvořit zálohu spuštěného správce front, záloha nemusí být konzistentní kvůli probíhajícím aktualizacím při kopírování souborů. Pokud je to možné, zastavte správce front spuštěním příkazu **endmqm -w** (ukončení čekání), pouze pokud se to nezdaří, použijte příkaz **endmqm -i** (okamžité ukončení).

Informace o této úloze

Chcete-li vytvořit záložní kopii dat správce front, postupujte takto:

Postup

1. Pomocí informací v konfiguračních souborech vyhledejte adresáře, do kterých správce front umísťuje svá data a soubory protokolu.

   Další informace viz téma “Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 83.

   Poznámka: Názvy, které se objevují v adresáři, jsou transformovány, aby se zajistilo, že jsou kompatibilní s platformou, na které používáte produkt IBM MQ. Další informace o transformacích názvů naleznete v tématu Základní informace o IBM MQ názvech souborů.
2. Pořídit kopie všech adresářů dat a souborů protokolu správce front včetně všech podadresářů.

   Ujistěte se, že nezmeškáte žádné soubory, zejména řídicí soubor protokolu, jak je popsáno v tématu “Jak vypadají protokoly” na stránce 622, a konfigurační soubory, jak je popsáno v tématu “Inicializační a konfigurační soubory” na stránce 236. Některé adresáře mohou být prázdné, ale potřebujete je všechny, abyste později obnovili zálohu.

   V případě kruhového protokolování zálohujte současně data správce front a adresáře souborů protokolu, abyste mohli obnovit konzistentní sadu dat a protokolů správce front.

   V případě lineárního protokolování zálohujte současně data správce front a adresáře souborů protokolu. Je možné obnovit pouze datové soubory správce front, pokud je k dispozici odpovídající úplná posloupnost souborů protokolu.
3. Zachovejte vlastnictví souborů.

   Linux AIX Pro systémy IBM MQ for UNIX a Linux to můžete provést pomocí příkazu **tar** . (Pokud máte fronty větší než 2 GB, nemůžete použít příkaz **tar** . Další informace naleznete v tématu Povolení velkých front.

Poznámka: Při upgradu na verzi IBM WebSphere MQ 7.5 a novější se ujistěte, že jste vytvořili zálohu souboru `qm.ini` a položek registru. Informace o správci front jsou uloženy v souboru `qm.ini` a lze je použít k návratu na předchozí verzi produktu IBM MQ.

Související úlohy

Zastavení správce front

"Zálohování konfiguračních souborů po vytvoření správce front" na stránce 14

Informace o konfiguraci systému IBM MQ jsou uloženy v konfiguračních souborech na systému AIX, Linux, and Windows. Po vytvoření správce front zazálohujte konfigurační soubory. Pokud pak vytvoříte jiného správce front, který způsobí problémy, můžete po odebrání zdroje problému obnovit zálohy.

Obnovení dat správce front

Chcete-li obnovit zálohu dat správce front, postupujte takto.

Než začnete

Před spuštěním zálohy se ujistěte, že není spuštěn správce front.

Při obnově zálohy správce front v klastru viz "Obnova správce front klastru" na stránce 360 a Klastrování: Dostupnost, více instancí a zotavení z havárie , kde získáte další informace.

Poznámka: Při upgradu na novější verzi produktu IBM MQse ujistěte, že jste vytvořili zálohu souboru **`.ini`** a položek registru. Informace o správci front jsou uloženy v souboru **`.ini`** a lze je použít k návratu na předchozí verzi produktu IBM MQ.

Postup

1. Pomocí informací v konfiguračních souborech vyhledejte adresáře, do kterých správce front umisťuje svá data a soubory protokolu.
2. Vyprázdněte adresáře, do kterých se chystáte umístit zálohovaná data.
3. Zkopírujte zálohovaná data správce front a soubory protokolu na správná místa.

   Ujistěte se, že máte řídicí soubor protokolu i soubory protokolu.

   V případě kruhového protokolování zálohujte současně data správce front a adresáře souborů protokolu, abyste mohli obnovit konzistentní sadu dat a protokolů správce front.

   V případě lineárního protokolování zálohujte současně data správce front a adresáře souborů protokolu. Je možné obnovit pouze datové soubory správce front, pokud je k dispozici odpovídající úplná posloupnost souborů protokolu.
4. Aktualizujte soubory s informacemi o konfiguraci.

   Zkontrolujte, zda jsou konfigurační soubory IBM MQ a správce front konzistentní, aby mohl produkt IBM MQ vyhledat obnovená data na správných místech.
5. Zkontrolujte výslednou adresářovou strukturu, abyste se ujistili, že máte všechny požadované adresáře.

   Další informace o adresářích a podadresářích systému IBM MQ naleznete v tématu Adresářová struktura na systémech Windows a v tématu Obsah adresáře na systémech AIX and Linux.

Výsledky

Pokud byla data správně zálohována a obnovena, bude nyní spuštěn správce front.

Multi Zálohování konfigurace správce front

Zálohování konfigurace správce front vám může pomoci znovu sestavit správce front z jeho definic, pokud dojde ke ztrátě konfigurace správce front i dat protokolu v důsledku selhání hardwaru a správce front nelze restartovat nebo obnovit z protokolu.

Informace o této úloze

ALW V systému AIX, Linux, and Windowsmůžete pomocí příkazu **dmpmqcfg** vypsat konfiguraci správce front IBM MQ .

IBM i V systému IBM imůžete pomocí příkazu Výpis MQ Configuration (**DMPMQMCFG**) vypsat objekty konfigurace a oprávnění pro správce front.

Postup

1. Ověřte, že je spuštěn správce fronty.
2. V závislosti na vaší platformě použijte jeden z následujících příkazů k zálohování konfigurace správce front:
   - ALW V systému AIX, Linux, and Windows: Proveďte příkaz Konfigurace výpisu MQ **dmpmqcfg**s použitím výchozí volby formátování (-f mqsc) MQSC a všech atributů (-a), pomocí standardního přesměrování výstupu uložte definice do souboru. Příklad:

     ```
     dmpmqcfg -m MYQMGR -a > /mq/backups/MYQMGR.mqsc
     ```

   - IBM i V systému IBM i: Spusťte příkaz pro výpis MQ Configuration (**DMPMQMCFG**) pomocí výchozí volby formátování OUTPUT (*MQSC) a EXPATTR (*ALL), použijte TOFILE a TOMBR k uložení definic do členu fyzického souboru. Příklad:

     ```
     DMPMQMCFG MQMNAME(MYQMGR) OUTPUT(*MQSC) EXPATTR(*ALL) TOFILE(QMQMSAMP/QMQSC)
     TOMBR(MYQMGRDEF)
     ```

Související úlohy

“Obnovení konfigurace správce front” na stránce 653
Konfiguraci správce front můžete obnovit ze zálohy tak, že se nejprve ujistíte, že je správce front spuštěn, a poté spustíte příslušný příkaz pro vaši platformu.

Související odkazy

dmpmqcfg (výpis konfigurace správce front)
Konfigurace výpisu paměti produktu MQ (DMPMQMCFG)

Multi Obnovení konfigurace správce front

Konfiguraci správce front můžete obnovit ze zálohy tak, že se nejprve ujistíte, že je správce front spuštěn, a poté spustíte příslušný příkaz pro vaši platformu.

Informace o této úloze

ALW V systému AIX, Linux, and Windowsmůžete pomocí příkazu **runmqsc** obnovit konfiguraci správce front IBM MQ .

IBM i V systému IBM imůžete pomocí příkazu **STRMQMMQSC** obnovit objekty konfigurace a oprávnění pro správce front.

Postup

1. Ověřte, že je spuštěn správce fronty.

   Všimněte si, že pokud je poškození dat a protokolů nezotavitelné jinými prostředky, mohl být správce front znovu vytvořen.
2. V závislosti na platformě obnovte konfiguraci správce front pomocí jednoho z následujících příkazů:

- ALW V systému AIX, Linux, and Windowsspusťte pro správce front příkaz **runmqsc** a pomocí standardního přesměrování vstupu obnovte definice ze skriptového souboru vygenerovaného příkazem Výpis MQ Configuration (**dmpmqcfg**) (viz “Zálohování konfigurace správce front” na stránce 652). Příklad:

  ```
  runmqsc MYQMGR < /mq/backups/MYQMGR.mqsc
  ```

- IBM i V systému IBM i: Spusťte **STRMQMMQSC** pro správce front a pomocí parametrů **SRCMBR** a **SRCFILE** obnovte definice ze člena fyzického souboru vygenerovaného příkazem Výpis MQ Configuration (**DMPMQMCFG**) (viz “Zálohování konfigurace správce front” na stránce 652). Příklad:

  ```
  STRMQMMQSC MQMNAME(MYQMGR) SRCFILE(QMQMSAMP/QMQSC) SRCMBR(MYQMGR)
  ```

Související úlohy

“Zálohování konfigurace správce front” na stránce 652
Zálohování konfigurace správce front vám může pomoci znovu sestavit správce front z jeho definic, pokud dojde ke ztrátě konfigurace správce front i dat protokolu v důsledku selhání hardwaru a správce front nelze restartovat nebo obnovit z protokolu.

Související odkazy

dmpmqcfg (výpis konfigurace správce front)
runmqsc (spuštění příkazů MQSC)
Konfigurace výpisu paměti produktu MQ (DMPMQMCFG)
Příkazy pro spuštění IBM MQ (STRMQMMQSC)

Použití záložního správce front

Existující správce front může mít vyhrazeného záložního správce front pro účely zotavení z havárie.

Informace o této úloze

Záložní správce front je neaktivní kopií existujícího správce front. Pokud se existující správce front stane neobnovitelným v důsledku závažného selhání hardwaru, může být záložní správce front převeden do stavu online, aby nahradil neobnovitelného správce front.

Existující soubory protokolu správce front musí být pravidelně kopírovány do záložního správce front, aby bylo zajištěno, že záložní správce front zůstane efektivní metodou zotavení z havárie. Existující správce front nemusí být zastaven, aby bylo možné soubory protokolu kopírovat, měli byste však soubor protokolu zkopírovat pouze v případě, že do něj správce front dokončil zápis. Informace o tom, jak zajistit, aby do konkrétního souboru protokolu již nebyl zapisován, viz “Aktualizace záložního správce front” na stránce 655 , aby jej bylo možné bezpečně zkopírovat.

Poznámka: Vzhledem k tomu, že existující protokol správce front je průběžně aktualizován, vždy existuje mírný nesoulad mezi existujícím protokolem správce front a daty protokolu zkopírovanými do záložního protokolu správce front. Pravidelné aktualizace správce front zálohy minimalizují nesoulad mezi těmito dvěma protokoly.

Pokud je vyžadováno, aby byl záložní správce front uveden do stavu online, musí být aktivován a poté spuštěn. Požadavek na aktivaci záložního správce front před jeho spuštěním je preventivním opatřením na ochranu proti náhodnému spuštění záložního správce front. Po aktivaci záložního správce front již nelze aktualizovat.

Důležité: Jakmile se starý záložní správce front stane novým aktivním správcem front, z jakéhokoli důvodu již nebude existovat záložní správce front. Jedná se o formu asynchronní replikace, a proto se očekává, že nový aktivní správce front bude logicky nějaký čas za starým aktivním správcem front. Starý aktivní správce front tak již nebude fungovat jako záloha pro nového aktivního správce front.

Procedura

- Informace o použití záložního správce front naleznete v následujících tématech:
  - “Vytvoření záložního správce front” na stránce 655
  - “Aktualizace záložního správce front” na stránce 655
  - “Spuštění záložního správce front” na stránce 656

Související pojmy

“Protokolování: Ujistěte se, že zprávy nejsou ztraceny” na stránce 621
Produkt IBM MQ zaznamenává všechny významné změny trvalých dat řízených správcem front do protokolu pro zotavení.

Vytvoření záložního správce front

Vytvoříte záložního správce front jako neaktivní kopii existujícího správce front.

Informace o této úloze

Důležité: Záložního správce front lze použít pouze při použití lineárního protokolování.

Záložní správce front vyžaduje následující:

- Chcete-li mít stejné atributy jako existující správce front, například název správce front, typ protokolování a velikost souboru protokolu.
- Chcete-li být na stejné platformě jako existující správce front.
- Chcete-li být na stejné nebo vyšší úrovni kódu než existující správce front.

Postup

1. Vytvořte záložního správce front pro existujícího správce front pomocí řídicího příkazu **crtmqm**.
2. Vytvořte kopie všech existujících adresářů dat a souborů protokolu správce front, včetně všech podadresářů, jak je popsáno v tématu “Zálohování dat správce front” na stránce 651.
3. Přepsat adresáře dat a souborů protokolu záložního správce front, včetně všech podadresářů, kopiemi převzatými z existujícího správce front.
4. Spusťte řídicí příkaz **strmqm** na záložním správci front, jak ukazuje následující příklad:

   ```
   strmqm -r BackupQMName
   ```

   Tento příkaz označí správce front jako záložního správce front v rámci produktu IBM MQa přehraje všechny zkopírované oblasti protokolu, aby přenesl záložního správce front v kroku s existujícím správcem front.

Související odkazy

crtmqm (vytvořit správce front)
strmqm (spustit správce front)

Aktualizace záložního správce front

Chcete-li zajistit, aby záložní správce front zůstal efektivní metodou zotavení z havárie, musí být pravidelně aktualizován.

Informace o této úloze

Pravidelná aktualizace zmenšuje nesoulad mezi záložním protokolem správce front a aktuálním protokolem správce front. Před jeho zálohováním není nutné správce front zastavit.

Upozornění: Pokud zkopírujete nesouvislou sadu protokolů do záložního adresáře protokolů správce front, budou přehrány pouze protokoly až do bodu, kde byl nalezen první chybějící protokol.

Postup

1. Ve správci front, který má být zálohován, zadejte následující příkaz skriptu (MQSC):

   ```
   RESET QMGR TYPE(ADVANCELOG)
   ```

   Tímto se zastaví jakýkoli zápis do aktuálního protokolu a poté se protokolování správce front přesune do další oblasti protokolu. Tím zajistíte, že zazálohujete všechny informace zaprotokolované do aktuálního času.
2. Získejte (nové) číslo oblasti aktuálního aktivního protokolu zadáním následujícího příkazu skriptu (MQSC) pro správce front, který má být zálohován:

   ```
   DIS QMSTATUS CURRLOG
   ```
3. Zkopírujte aktualizované soubory oblastí protokolu z aktuálního adresáře protokolů správce front do záložního adresáře protokolů správce front.

   Zkopírujte všechny oblasti protokolu od poslední aktualizace a až (ale ne včetně) aktuální oblasti uvedené v souboru “2” na stránce 656. Zkopírujte pouze soubory rozsahu protokolu, které začínají na "S...".
4. Spusťte řídicí příkaz **strmqm** na záložním správci front, jak ukazuje následující příklad:

   ```
   strmqm -r BackupQMName
   ```

   Tato akce přehraje všechny zkopírované oblasti protokolu a přenese záložního správce front do kroku se správcem front. Po dokončení přehrání obdržíte zprávu, která identifikuje všechny oblasti protokolu potřebné pro zotavení při restartu a všechny oblasti protokolu potřebné pro zotavení z médií.

Související odkazy
RESET QMGR
ZOBRAZENÍ QMSTATUS
strmqm (spustit správce front)

Spuštění záložního správce front

Můžete nahradit záložního správce front pro nezotavitelného správce front.

Informace o této úloze

Při obnově zálohy správce front v klastru viz “Obnova správce front klastru” na stránce 360 a Klastrování: Dostupnost, více instancí a zotavení z havárie , kde získáte další informace.

Pokud má neobnovitelný správce front vyhrazeného záložního správce front, můžete jej aktivovat namísto neobnovitelného správce front.

Je-li neobnovitelný správce front nahrazen záložním správcem front, mohou být některá data správce front z neobnovitelného správce front ztracena. Množství ztracených dat závisí na tom, jak nedávno byl zálohovací správce front naposledy aktualizován. Čím novější je poslední aktualizace, tím menší je ztráta dat správce front.

Poznámka: I když jsou data správce front a soubory protokolu uloženy v různých adresářích, ujistěte se, že zálohujete a obnovíte adresáře současně. Pokud mají data správce front a soubory protokolu různé stáří, není správce front v platném stavu a pravděpodobně nebude spuštěn. I když se spustí, vaše data budou pravděpodobně poškozena.

Postup

1. Spuštěním řídicího příkazu **strmqm** aktivujte záložního správce front, jak ukazuje následující příklad:

   ```
   strmqm -a BackupQMName
   ```

   Záložní správce front je aktivován. Nyní, když je aktivní, nelze již aktualizovat záložního správce front.

2. Spuštěním řídicího příkazu **strmqm** spusťte záložní správce front, jak je uvedeno v následujícím příkladu:

   ```
   strmqm BackupQMName
   ```

   Produkt IBM MQ to považuje za obnovení po restartu a používá protokol ze záložního správce front. Během poslední aktualizace záložního správce front došlo k přehrání, a proto jsou odvolány pouze aktivní transakce z posledního zaznamenaného kontrolního bodu.
3. Restartujte všechny kanály.
4. Zkontrolujte výslednou adresářovou strukturu, abyste se ujistili, že máte všechny požadované adresáře.

   Další informace o adresářích a podadresářích systému IBM MQ naleznete v tématu Plánování podpory systému souborů.
5. Ujistěte se, že máte řídicí soubor protokolu i soubory protokolu. Také zkontrolujte, zda jsou konfigurační soubory IBM MQ a správce front konzistentní, aby mohl produkt IBM MQ hledat obnovená data na správných místech.

Výsledky

Pokud byla data správně zálohována a obnovena, spustí se nyní správce front.

Související úlohy

“Restartování zastavených kanálů” na stránce 229
Když kanál přejde do stavu ZASTAVENO, musíte kanál restartovat ručně.

Související odkazy

strmqm (spustit správce front)

Změny zotavení z chyb klastru (na jiných serverech než z/OS)

Správce front znovu provádí operace, které způsobily problémy, dokud nejsou problémy vyřešeny. Pokud se po pěti dnech problémy nevyřeší, správce front se vypne, aby se zabránilo dalšímu zastarávání mezipaměti.

Správce front znovu provádí operace, které způsobily problémy, dokud nejsou problémy vyřešeny. Pokud se po pěti dnech problémy nevyřeší, správce front se vypne, aby se zabránilo dalšímu zastarávání mezipaměti. Vzhledem k tomu, že mezipaměť je více zastaralá, způsobuje větší počet problémů. Toto chování týkající se chyb klastru se nevztahuje na z/OS.

Každý aspekt správy klastrů je pro správce front zpracováván procesem lokálního správce úložiště `amqrrmfa`. Proces se spustí ve všech správcích front, i když neexistují žádné definice klastrů.

IBM MQ, spíše než zastavovat správce úložiště a pokračovat bez něj, správce úložiště znovu provádí nezdařené operace. Pokud správce front zjistí problém se správcem úložiště, provede jeden ze dvou kroků.

1. Pokud chyba neohrozí činnost správce front, správce front zapíše zprávu do protokolu chyb. Znovu provede operaci, která selhala, každých 10 minut, dokud nebude operace úspěšná. Při výchozím nastavení máte pět dní na to, abyste se s touto chybou vypořádali. Při selhání správce front zapíše zprávu do protokolu chyb a vypne se. Můžete odložit pětidenní vypnutí.
2. Pokud chyba ohrožuje činnost správce front, zapíše správce front zprávu do protokolu chyb a okamžitě se vypne.

Chyba, která ohrožuje činnost správce front, je chyba, kterou správce front nemohl diagnostikovat, nebo chyba, která může mít nepředvídatelné důsledky. Tento typ chyby často vede k tomu, že správce front zapíší soubor FFST . Chyby, které ohrožují činnost správce front, mohou být způsobeny chybou v IBM MQnebo administrátorem či programem, který provádí neočekávané akce, například ukončení procesu IBM MQ .

Bodem změny chování při zotavení z chyb je omezení času, po který bude správce front nadále pracovat, s rostoucím počtem nekonzistentních definic klastrů. S rostoucím počtem nekonzistencí v definicích klastru roste pravděpodobnost nestandardního chování aplikace.

Výchozí volba vypnutí správce front po pěti dnech je kompromisem mezi omezením počtu nekonzistencí a zachováním dostupnosti správce front, dokud nebudou problémy zjištěny a vyřešeny.

Dobu před ukončením činnosti správce front můžete prodloužit na neomezenou dobu, než opravíte problém nebo počkáte na plánované ukončení práce správce front. Pětidenní pobyt udržuje správce front v chodu přes prodloužený víkend, což vám dává čas reagovat na případné problémy nebo prodloužit dobu před restartováním správce front.

Nápravná opatření

Máte na výběr akce, které se zabývají problémy s obnovou chyb klastru. První volbou je monitorovat a opravit problém a druhá monitorovat a odložit opravu problému.

1. Monitorujte protokol chyb správce front pro chybové zprávy AMQ9448 a AMQ5008a opravte problém.

   AMQ9448 označuje, že správce úložiště vrátil chybu po spuštění příkazu. Tato chyba označuje začátek opakování příkazu každých 10 minut a případně zastavení správce front po pěti dnech, pokud neodložíte ukončení práce systému.
   AMQ5008 označuje, že správce front byl zastaven, protože chybí proces IBM MQ . AMQ5008 výsledky zastavení správce úložiště po pěti dnech. Pokud se správce úložiště zastaví, zastaví se.
2. Monitorujte protokol chyb správce front pro chybovou zprávu AMQ9448a odložte opravu problému.

   Pokud zakážete získávání zpráv z produktu `SYSTEM.CLUSTER.COMMAND.QUEUE`, správce úložiště se přestane pokoušet spouštět příkazy a bude pokračovat po neomezenou dobu bez zpracování jakékoli práce. Všechny manipulátory, které správce úložiště zadrží pro fronty, jsou však uvolněny. Vzhledem k tomu, že se správce front nezastaví, nebude zastaven po pěti dnech.
   Spuštěním příkazu MQSC zakážete získávání zpráv z produktu `SYSTEM.CLUSTER.COMMAND.QUEUE`:
   ```
   ALTER QLOCAL(SYSTEM.CLUSTER.COMMAND.QUEUE) GET(DISABLED)
   ```
   Chcete-li obnovit příjem zpráv z produktu `SYSTEM.CLUSTER.COMMAND.QUEUE` , spusťte příkaz MQSC:
   ```
   ALTER QLOCAL(SYSTEM.CLUSTER.COMMAND.QUEUE) GET(ENABLED)
   ```

Zvláštní pozornost

Zastavení `amqrrmfa` v IBM MQ způsobí zastavení správce front, protože je považován za selhání správce front. Proces `amqrrmfa` nesmíte zastavit, pokud nenastavíte parametr ladění správce front `TolerateRepositoryFailure`.

Příklad

```
TuningParameters:
        TolerateRepositoryFailure=TRUE
```

Obrázek 86. V souboru qm.ini nastavte hodnotu `TolerateRepositoryFailure` na TRUE .

Související pojmy

“Konfigurační soubory správce front, qm.ini” na stránce 97
Konfigurační soubor správce front `qm.ini`obsahuje informace týkající se konkrétního správce front. Atributy, které můžete použít k úpravě konfigurace jednotlivého správce front, přepíší veškerá nastavení pro produkt IBM MQ.

Konfigurace prostředků JMS a Jakarta Messaging

Jedním ze způsobů, jak může aplikace JMS nebo Jakarta Messaging vytvořit a nakonfigurovat prostředky, které potřebuje pro připojení k produktu IBM MQ , a přistupovat k místům určení pro odesílání nebo příjem zpráv, je použití rozhraní JNDI (Java Naming and Directory Interface) k načtení spravovaných

objektů z umístění v rámci služby pojmenování a adresářové služby, která se nazývá obor názvů JNDI. Než bude aplikace JMS moci načíst spravované objekty z oboru názvů JNDI, musíte nejprve vytvořit a nakonfigurovat spravované objekty.

Informace o této úloze

V 9.3.0 JM 3.0 V 9.3.0 Od IBM MQ 9.3.0, Jakarta Messaging 3.0 je podporován pro vývoj nových aplikací. Produkt IBM MQ 9.3.0 nadále podporuje produkt JMS 2.0 pro existující aplikace. Použití rozhraní API Jakarta Messaging 3.0 a rozhraní API JMS 2.0 ve stejné aplikaci není podporováno. Další informace naleznete v tématu Použití tříd IBM MQ pro systém zpráv JMS/Jakarta.

Spravované objekty v produktu IBM MQ můžete vytvářet a konfigurovat pomocí jednoho z následujících nástrojů:

Nástroje pro administraci produktu IBM MQ JMS a Jakarta Messaging
Nástroj pro administraci IBM MQ JMS **JMSAdmin**a Jakarta Messaging administration tool, **JMS30Admin**jsou nástroje příkazového řádku, které můžete použít k vytvoření a konfiguraci objektů IBM MQ JMS a Jakarta Messaging , které jsou uloženy v LDAP, v lokálním systému souborů nebo v jiných umístěních. Nástroje pro administraci JMS a Jakarta Messaging používají syntaxi, která je podobná syntaxi **runmqsc**, a také podporují skriptování.

Administrační nástroje používají konfigurační soubor k nastavení hodnot určitých vlastností. Je dodán ukázkový konfigurační soubor, který můžete upravit tak, aby vyhovoval vašemu systému, než začnete pomocí nástroje pro konfiguraci prostředků JMS . Další informace o konfiguračním souboru viz téma “Konfigurace nástrojů JMSAdmin a JMS30Admin” na stránce 666.

JMS 2.0 **IBM MQ Explorer**
Pro systém JMS 2.0můžete použít produkt IBM MQ Explorer k vytvoření a správě definic objektů JMS 2.0 , které jsou uloženy v LDAP, v lokálním systému souborů nebo v jiných umístěních.

V 9.3.0 JM 3.0 V 9.3.0 Pro Jakarta Messaging 3.0nemůžete spravovat rozhraní JNDI pomocí IBM MQ Explorer. Administrace rozhraní JNDI je podporována Jakarta Messaging 3.0 variantou **JMSAdmin**, což je **JMS30Admin**.

Aplikace IBM MQ JMS , které jsou implementovány do WebSphere Application Server , potřebují přístup k objektům JMS z úložiště JNDI aplikačního serveru. Proto, pokud používáte systém zpráv JMS mezi WebSphere Application Server a IBM MQ, musíte vytvořit objekty v produktu WebSphere Application Server , které odpovídají objektům, které jste vytvořili v produktu IBM MQ.

V 9.3.0 JM 3.0 V 9.3.0 Ačkoli IBM MQ 9.3 podporuje Jakarta Messaging 3.0, WebSphere Application Server momentálně nemá ekvivalentní podporu. Proto v produktu WebSphere Application Serverkonfigurujete prostředky Java Message Service 2.0 .

Produkt IBM MQ Explorer a nástroj pro administraci produktu IBM MQ JMS nelze použít k administraci objektů produktu IBM MQ JMS , které jsou uloženy v adresáři WebSphere Application Server. Místo toho můžete vytvořit a nakonfigurovat spravované objekty v produktu WebSphere Application Server pomocí jednoho z následujících nástrojů:

WebSphere Application Server Administrativní konzola
Administrativní konzola WebSphere Application Server je webový nástroj, který lze použít ke správě objektů produktu IBM MQ JMS v produktu WebSphere Application Server.

WebSphere Application Server skriptovací klient wsadmin
Skriptovací klient WebSphere Application Server wsadmin poskytuje specializované příkazy pro administraci objektů IBM MQ JMS v produktu WebSphere Application Server.

Chcete-li použít aplikaci JMS pro přístup k prostředkům správce front IBM MQ z produktu WebSphere Application Server, musíte použít poskytovatele systému zpráv IBM MQ v adresáři WebSphere Application Server, který obsahuje verzi produktu IBM MQ classes for JMS. Adaptér prostředků IBM MQ dodávaný s produktem WebSphere Application Server je používán všemi aplikacemi, které provádějí systém zpráv JMS s poskytovatelem systému zpráv IBM MQ . Adaptér prostředků IBM MQ se obvykle aktualizuje automaticky při použití opravných sad WebSphere Application Server , ale pokud jste dříve ručně

aktualizovali adaptér prostředků, musíte ručně aktualizovat konfiguraci, abyste se ujistili, že je údržba správně použita.

Související pojmy

Vytvoření a konfigurace továren připojení a míst určení ve třídách IBM MQ pro aplikaci JMS

Související odkazy

runmqsc (spuštění příkazů MQSC)

Konfigurace továren připojení a míst určení v oboru názvů rozhraní JNDI

Aplikace JMS a Jakarta Messaging přistupují ke spravovaným objektům ve službě pro správu pojmenování a adresářů prostřednictvím rozhraní JNDI (Java Naming and Directory Interface). Spravované objekty JMS nebo Jakarta Messaging jsou uloženy v umístění v rámci služby pro správu pojmenování a adresářů, která se nazývá obor názvů JNDI. Aplikace JMS nebo Jakarta Messaging může vyhledat spravované objekty pro připojení k produktu IBM MQ a přistupovat k místům určení pro odesílání nebo příjem zpráv.

Informace o této úloze

Aplikace JMS nebo Jakarta Messaging vyhledají názvy objektů JMS nebo Jakarta Messaging ve službě pro správu pojmenování a adresářů pomocí kontextů:

počáteční kontext
Počáteční kontext definuje kořen oboru názvů JNDI. Pro každé umístění ve službě pro správu pojmenování a adresářů musíte zadat počáteční kontext, který poskytne počáteční bod, ze kterého může aplikace JMS nebo Jakarta Messaging interpretovat názvy spravovaných objektů v tomto umístění služby pro správu pojmenování a adresářů.

Dílčí kontexty
Kontext může mít jeden nebo více dílčích kontextů. Dílčí kontext je subdivize oboru názvů rozhraní JNDI a může obsahovat spravované objekty, jako jsou továrny připojení a místa určení, stejně jako další dílčí kontexty. Dílčí kontext není sám o sobě objektem. Je pouze rozšířením konvence pojmenování objektů v dílčím kontextu.

Než bude moci aplikace IBM MQ classes for JMS nebo IBM MQ classes for Jakarta Messaging načíst spravované objekty z oboru názvů rozhraní JNDI, musíte nejprve vytvořit spravované objekty. Můžete vytvořit a nakonfigurovat následující typy objektů JMS nebo Jakarta Messaging :

Továrna připojení
Objekt továrny připojení JMS nebo Jakarta Messaging definuje sadu standardních vlastností konfigurace pro připojení. Aplikace JMS nebo Jakarta Messaging používá továrnu připojení k vytvoření připojení k produktu IBM MQ. Můžete vytvořit továrnu připojení, která je specifická pro jednu ze dvou domén systému zpráv, doménu systému zpráv typu point-to-point a doménu systému zpráv publikování/odběru.

Případně můžete z produktu JMS 1.1vytvořit továrny připojení nezávislé na doméně, které lze použít pro systém zpráv typu point-to-point i publikování/odběr. Další informace viz Model systému zpráv JMS a Jakarta.

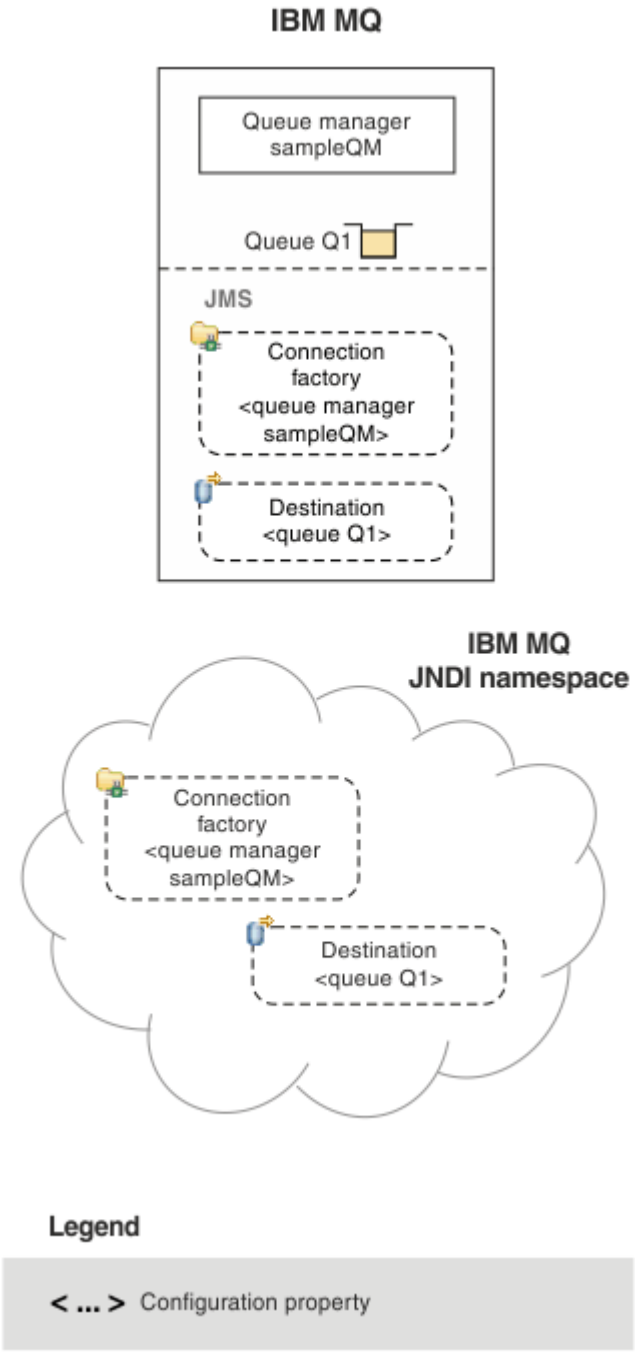
Místo určení
Cíl JMS nebo Jakarta Messaging je objekt, který představuje cíl zpráv, které klient produkuje, a zdroj zpráv, které aplikace JMS spotřebovává. Aplikace JMSnebo Jakarta Messaging může buď použít jeden cílový objekt k vložení zpráv a k získání zpráv, nebo může použít samostatné cílové objekty. Existují dva typy cílového objektu:

- Cíl fronty JMS nebo Jakarta Messaging používaný v systému zpráv typu point-to-point
- JMS nebo Jakarta Messaging místo určení tématu použité v systému zpráv publikování/odběru

JMS 2.0 Pro systém JMS 2.0můžete vytvářet kontexty a spravované objekty buď pomocí nástroje IBM MQ Explorer , nebo pomocí nástroje pro administraci IBM MQ JMS **JMSAdmin**.

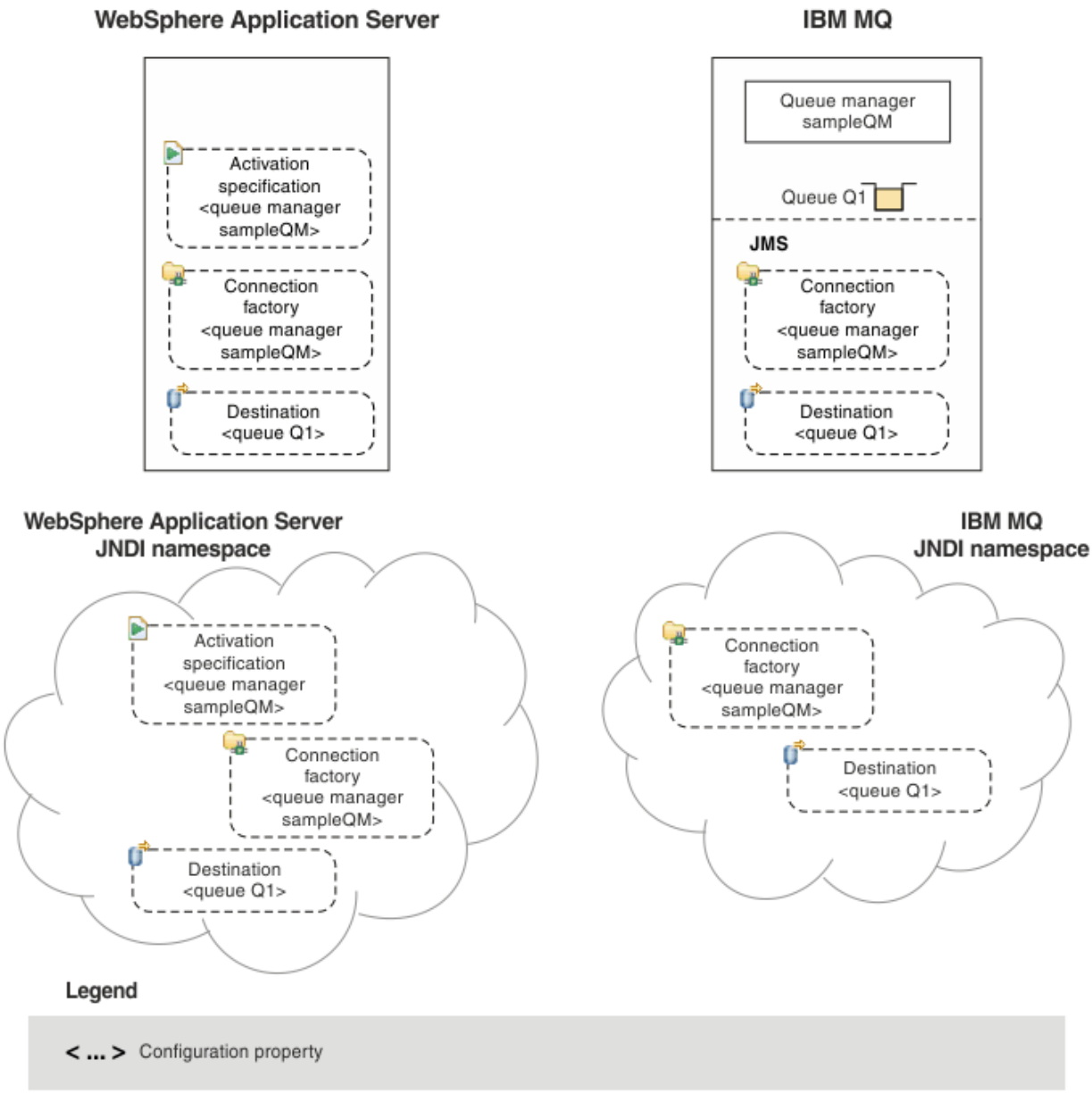
Poznámka: V 9.3.0 JM 3.0 V 9.3.0 Pro Jakarta Messaging 3.0nemůžete spravovat rozhraní JNDI pomocí IBM MQ Explorer. Administrace rozhraní JNDI je podporována Jakarta Messaging 3.0 variantou **JMSAdmin**, což je **JMS30Admin**.

Následující diagram zobrazuje příklad objektů JMS nebo Jakarta Messaging vytvořených v oboru názvů rozhraní JNDI IBM MQ .



Obrázek 87. JMS nebo Jakarta Messaging objekty vytvořené v IBM MQ

Pokud používáte systém zpráv JMS mezi WebSphere Application Server a IBM MQ, musíte vytvořit odpovídající objekty v produktu WebSphere Application Server , které se použijí ke komunikaci s produktem IBM MQ. Když vytvoříte jeden z těchto objektů v produktu WebSphere Application Server, je uložen v oboru názvů rozhraní JNDI produktu WebSphere Application Server , jak ukazuje následující diagram.



Obrázek 88. Objekty vytvořené v adresáři WebSphere Application Servera odpovídající objekty v adresáři IBM MQ

V 9.3.0 JM 3.0 V 9.3.0 Ačkoli IBM MQ 9.3 podporuje Jakarta Messaging 3.0, WebSphere Application Server momentálně nemá ekvivalentní podporu. Proto v produktu WebSphere Application Serverkonfigurujete prostředky Java Message Service 2.0 .

Pokud vaše aplikace používá objekt typu message-driven bean (MDB), továrna připojení se používá pouze pro odchozí zprávy a příchozí zprávy jsou přijímány specifikací aktivace. Specifikace aktivace jsou součástí standardu Java EE Connector Architecture 1.5 (JCA 1.5). Produkt JCA 1.5 poskytuje standardní způsob integrace poskytovatelů produktu JMS , jako např. IBM MQ, s aplikačními servery Java EE , jako např. WebSphere Application Server. Specifikace aktivace JMS může být přidružena k jednomu nebo více objektům typu message-driven bean (MDB) a poskytuje konfiguraci nezbytnou pro to, aby tyto objekty MDB naslouchaly zprávám přicházejícím do místa určení.

K vytvoření a konfiguraci prostředků JMS , které potřebujete, můžete použít buď administrativní konzolu WebSphere Application Server , nebo skriptovací příkazy wsadmin.

Procedura

- JMS 2.0
  Chcete-li nakonfigurovat objekty JMS pro IBM MQ pomocí IBM MQ Explorer, viz “Konfigurace objektů JMS 2.0 pomocí IBM MQ Explorer” na stránce 663.
- JMS 2.0
  Chcete-li konfigurovat objekty JMS pro systém IBM MQ pomocí nástroje pro administraci IBM MQ JMS , **JMSAdmin**, viz “Konfigurace objektů JMS a Jakarta Messaging pomocí nástrojů pro administraci” na stránce 664.
- V 9.3.0 JM 3.0 V 9.3.0
  Chcete-li konfigurovat objekty Jakarta Messaging pro systém IBM MQ pomocí nástroje pro administraci IBM MQ Jakarta Messaging , **JMS30Admin**, viz “Konfigurace objektů JMS a Jakarta Messaging pomocí nástrojů pro administraci” na stránce 664.
- JMS 2.0
  Chcete-li konfigurovat objekty JMS pro WebSphere Application Server, viz “Konfigurace prostředků JMS 2.0 v adresáři WebSphere Application Server” na stránce 674.

Výsledky

Aplikace IBM MQ classes for JMS nebo IBM MQ classes for Jakarta Messaging může načíst spravované objekty z oboru názvů JNDI a v případě potřeby nastavit nebo změnit jednu nebo více svých vlastností pomocí rozšíření IBM JMS nebo rozšíření IBM MQ JMS .

Související úlohy

Použití rozhraní JNDI k načtení spravovaných objektů v aplikaci JMS
Vytvoření a konfigurace továren připojení a míst určení v aplikaci IBM MQ classes for JMS

JMS 2.0 Konfigurace objektů JMS 2.0 pomocí IBM MQ Explorer

Grafické uživatelské rozhraní IBM MQ Explorer slouží k vytváření objektů JMS z objektů IBM MQ a objektů IBM MQ z objektů JMS a k administraci a monitorování jiných objektů IBM MQ .

Informace o této úloze

JMS 2.0 IBM MQ Explorer je grafické uživatelské rozhraní, ve kterém můžete spravovat a monitorovat objekty IBM MQ, ať je jejich hostitelem lokální počítač nebo vzdálený systém. IBM MQ Explorer běží na Windows a Linux for x86-64. Může se vzdáleně připojit ke správcům front, kteří jsou spuštěni na libovolné podporované platformě, včetně platformy z/OS, což umožňuje zobrazit, prozkoumat a změnit celou páteř systému zpráv z konzoly.

Poznámka: V 9.3.0 JM 3.0 V 9.3.0 Pro Jakarta Messaging 3.0nemůžete spravovat rozhraní JNDI pomocí IBM MQ Explorer. Administrace rozhraní JNDI je podporována Jakarta Messaging 3.0 variantou **JMSAdmin**, což je **JMS30Admin**.

V produktu IBM MQ Explorerjsou všechny továrny připojení uloženy ve složkách Továrny připojení v příslušném kontextu a dílčích kontextech.

S produktem IBM MQ Explorermůžete provádět následující typy úloh, a to buď kontextově z existujícího objektu v produktu IBM MQ Explorer, nebo z průvodce vytvořením nového objektu:

- Vytvořte továrnu připojení JMS z libovolného z následujících objektů IBM MQ :
  - Správce front IBM MQ , ať už v lokálním počítači nebo ve vzdáleném systému.
  - Kanál IBM MQ .
  - Modul listener IBM MQ .
- Přidejte správce front IBM MQ do produktu IBM MQ Explorer pomocí továrny připojení JMS .

- Vytvořte frontu JMS z fronty IBM MQ .
- Vytvořte frontu IBM MQ z fronty JMS .
- Vytvořte téma JMS z tématu IBM MQ , kterým může být objekt IBM MQ nebo dynamické téma.
- Vytvořte téma IBM MQ z tématu JMS .

Procedura

- Spusťte soubor IBM MQ Explorer, pokud ještě není spuštěn.

  Pokud je spuštěn produkt IBM MQ Explorer a zobrazuje úvodní stránku, zavřete úvodní stránku, abyste zahájili administraci objektů IBM MQ .
- Pokud jste tak dosud neučinili, vytvořte počáteční kontext definující kořen oboru názvů JNDI, ve kterém jsou objekty JMS uloženy ve službě pro správu pojmenování a adresářů.

  Po přidání počátečního kontextu do produktu IBM MQ Explorer můžete v oboru názvů JNDI vytvořit objekty továrny připojení, cílové objekty a dílčí kontexty.

  Počáteční kontext se zobrazí v pohledu Navigator ve složce Spravované objekty produktu JMS . Všimněte si, že ačkoli se zobrazuje úplný obsah oboru názvů rozhraní JNDI, v produktu IBM MQ Explorer můžete upravit pouze objekty IBM MQ classes for JMS , které jsou zde uloženy. Další informace naleznete v tématu Přidání počátečního kontextu.
- Vytvořte a nakonfigurujte dílčí kontexty a JMS spravované objekty, které potřebujete.

  Další informace naleznete v tématu Vytvoření a konfigurace JMS spravovaných objektů.
- Nakonfigurujte prostor IBM MQ.

  Další informace viz Konfigurace IBM MQ pomocí IBM MQ Explorer .

Související pojmy

Úvod do produktu IBM MQ Explorer

Vytvoření a konfigurace továren připojení a míst určení v aplikaci IBM MQ classes for JMS

Konfigurace objektů JMS a Jakarta Messaging pomocí nástrojů pro administraci

Produkt IBM MQ poskytuje nástroje pro administraci, které lze použít k definování vlastností osmi typů objektů IBM MQ classes for JMS nebo IBM MQ classes for Jakarta Messaging a k jejich uložení v oboru názvů rozhraní JNDI. Aplikace pak mohou použít rozhraní JNDI k načtení těchto spravovaných objektů z oboru názvů.

Informace o této úloze

JMS 2.0 V případě operačního systému JMS 2.0je administrace rozhraní JNDI podporována nástrojem **JMSAdmin** .

V 9.3.0 JM 3.0 V 9.3.0 V případě operačního systému Jakarta Messaging 3.0je administrace rozhraní JNDI podporována Jakarta Messaging 3.0 variantou **JMSAdmin**, což je **JMS30Admin**.

V následující tabulce je uvedeno osm typů spravovaných objektů, které můžete vytvářet, konfigurovat a manipulovat s nimi pomocí příkazových slov. Sloupec Klíčové slovo zobrazuje řetězce, které můžete nahradit za *TYPE* v příkazech uvedených v části Tabulka 36 na stránce 665.

Tabulka 36. Typy objektů JMS a Jakarta Messaging , které jsou zpracovány administračním nástrojem.		
Typ objektu	**Klíčové slovo**	**Popis**
MQConnectionFactory	CF	Implementace IBM MQ rozhraní JMS ConnectionFactory . Toto představuje objekt továrny pro vytváření připojení v doménách typu point-to-point i publikování/odběr.
Továrna MQQueueConnection	QCF-počet	Implementace IBM MQ rozhraní továrny JMS QueueConnection. Toto představuje objekt továrny pro vytváření připojení v doméně typu point-to-point.
Továrna MQTopicConnection	TCF-zařízení	Implementace IBM MQ rozhraní továrny JMS TopicConnection. Toto představuje objekt továrny pro vytváření připojení v doméně publikování/odběru.
MQQUEUE	Q	Implementace IBM MQ rozhraní fronty JMS . Toto představuje cíl pro zprávy v doméně typu point-to-point.
Téma MQTopic	T	Implementace IBM MQ rozhraní tématu JMS . Toto představuje cíl pro zprávy v doméně publikování/odběru.
MQXAConnectionFactory "1" na stránce 665	XACF	Implementace IBM MQ rozhraní JMS XAConnectionFactory . Toto představuje objekt továrny pro vytváření připojení v doménách typu point-to-point i publikování/odběr a v místech, kde připojení používají verze XA tříd JMS .
MQXAQueueConnectionTovárna "1" na stránce 665	XAQCF	Implementace IBM MQ rozhraní továrny JMS XAQueueConnection. Toto představuje objekt továrny pro vytváření připojení v doméně typu point-to-point, která používají verze XA tříd JMS .
MQXATopicConnectionTovárna "1" na stránce 665	XATCF	Implementace IBM MQ rozhraní továrny JMS XATopicConnection. Toto představuje objekt továrny pro vytváření připojení v doméně publikování/odběru, které používají verze XA tříd JMS .

Poznámka:

1. Tyto třídy jsou poskytovány pro použití dodavateli aplikačních serverů. Je nepravděpodobné, že by byly přímo užitečné pro aplikační programátory.

Další informace o konfiguraci těchto objektů viz "Konfigurace objektů JMS" na stránce 673.

Typy a hodnoty vlastností, které potřebujete k použití tohoto nástroje, jsou uvedeny v seznamu Vlastnosti IBM MQ classes for JMS objektů.

Tento nástroj můžete také použít k manipulaci s dílčími kontexty oboru názvů adresáře v rámci rozhraní JNDI, jak je popsáno v tématu "Konfigurace dílčích kontextů" na stránce 670.

JMS 2.0 Pro systém JMS 2.0 a starší můžete také vytvořit a nakonfigurovat IBM MQ classes for JMS spravované objekty pomocí IBM MQ Explorer.

V 9.3.0 JM 3.0 V 9.3.0 Pro Jakarta Messaging 3.0nemůžete spravovat rozhraní JNDI pomocí IBM MQ Explorer. Administrace rozhraní JNDI je podporována Jakarta Messaging 3.0 variantou **JMSAdmin**, což je **JMS30Admin**.

Související pojmy

Vytvoření a konfigurace továren připojení a míst určení v aplikaci IBM MQ classes for JMS

Použití rozhraní JNDI k načtení spravovaných objektů v aplikaci JMS

Konfigurace nástrojů JMSAdmin a JMS30Admin

Nástroje pro administraci produktu IBM MQ JMS a Jakarta Messaging používají konfigurační soubor k nastavení hodnot určitých vlastností. V každém případě je dodán ukázkový konfigurační soubor, který můžete upravit tak, aby vyhovoval vašemu systému.

Informace o této úloze

V 9.3.0 JM 3.0 V 9.3.0 IBM MQ 9.3.0 zavádí podporu pro produkt Jakarta Messaging 3.0. JMS 2.0 je stále plně podporován.

Konfigurační soubor je prostý textový soubor, který se skládá ze sady dvojic klíč-hodnota, oddělených rovnítkem (=). Nástroj pro administraci nakonfigurujete nastavením hodnot pro tři vlastnosti definované v konfiguračním souboru. Následující příklad ukazuje tyto tři vlastnosti:

```
#Set the service provider
INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
#Set the initial context
PROVIDER_URL=ldap://polaris/o=ibm_us,c=us
#Set the authentication type
SECURITY_AUTHENTICATION=none
```

V tomto příkladu znak křížku (#) v prvním sloupci řádku označuje komentář nebo řádek, který se nepoužívá.

Ukázkový konfigurační soubor, který se používá jako výchozí konfigurační soubor, je dodáván s produktem IBM MQ. Ukázkový soubor se nazývá `JMSAdmin.config` (pro JMS 2.0) nebo `JMS30Admin.config` (pro Jakarta Messaging 3.0). Tento soubor se nachází v adresáři *MQ_JAVA_INSTALL_PATH*`/bin` . Můžete buď upravit ukázkový soubor tak, aby definoval nastavení potřebná pro váš systém, nebo vytvořit vlastní konfigurační soubor.

Když spustíte nástroj pro administraci, můžete určit konfigurační soubor, který chcete použít, pomocí parametru příkazového řádku `-cfg` , jak je popsáno v tématu “Spuštění nástrojů JMSAdmin a JMS30Admin” na stránce 668. Pokud při vyvolání nástroje nezadáte název konfiguračního souboru, nástroj se pokusí načíst výchozí konfigurační soubor (`JMSAdmin.config` nebo `JMS30Admin.config`). Vyhledá tento soubor nejprve v aktuálním adresáři a poté v adresáři *MQ_JAVA_INSTALL_PATH*`/bin` , kde *MQ_JAVA_INSTALL_PATH* je cesta k vaší instalaci produktu IBM MQ classes for JMS nebo IBM MQ classes for Jakarta Messaging .

Názvy objektů JMS nebo Jakarta Messaging , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jednou z těchto konvencí je, že názvy objektů a kontextů musí obsahovat předponu, například `cn=` (obecný název) nebo `ou=` (organizační jednotka). Nástroj pro administraci zjednodušuje používání poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který zadáte. Pro LDAP se jedná o `cn=`. V případě potřeby můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru.

Poznámka: Možná budete muset nakonfigurovat server LDAP tak, aby ukládal objekty Java . Další informace naleznete v dokumentaci k serveru LDAP.

Postup

1. Definujte poskytovatele služeb, kterého nástroj používá, konfigurací vlastnosti **INITIAL_CONTEXT_FACTORY** .

   Podporované hodnoty pro tuto vlastnost jsou následující:

   - com.sun.jndi.ldap.LdapCtxFactory (pro LDAP)
   - com.sun.jndi.fscontext.RefFSContextFactory (pro kontext systému souborů)
   - z/OS com.ibm.jndi.LDAPCtxFactory je podporován pouze v systému z/OS a poskytuje přístup k serveru LDAP. Tato třída je však nekompatibilní s com.sun.jndi.ldap.LdapCtxFactoryv tom, že objekty vytvořené pomocí jedné továrny InitialContextnelze číst nebo upravovat pomocí druhé továrny.

   Můžete také použít nástroj administrace pro připojení k jiným kontextům rozhraní JNDI pomocí tří parametrů definovaných v konfiguračním souboru JMSAdmin nebo JMS30Admin . Chcete-li použít jinou továrnu InitialContext, postupujte takto:

   a) Nastavte vlastnost **INITIAL_CONTEXT_FACTORY** na požadovaný název třídy.

   b) Definujte chování továrny InitialContextpomocí vlastností **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** a **NAME_READABILITY_MARKER** .

      Nastavení těchto vlastností jsou popsána v komentářích ukázkového konfiguračního souboru.

   Pokud použijete jednu z podporovaných hodnot **INITIAL_CONTEXT_FACTORY** , nemusíte definovat vlastnosti **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** a **NAME_READABILITY_MARKER** . Těmto vlastnostem však můžete poskytnout hodnoty, chcete-li přepsat předvolby systému. Pokud jsou například objekty uloženy v prostředí LDAP, můžete změnit výchozí předponu, kterou nástroj přidá k názvům objektů a kontextů, nastavením vlastnosti **NAME_PREFIX** na požadovanou předponu.

   Pokud vynecháte jednu nebo více ze tří vlastností továrny InitialContext, nástroj pro administraci poskytne vhodné výchozí hodnoty na základě hodnot ostatních vlastností.

2. Definujte URL počátečního kontextu relace konfigurací vlastnosti **PROVIDER_URL** .

   Tato URL je kořenovým adresářem všech operací rozhraní JNDI prováděných nástrojem. Podporovány jsou dvě formy této vlastnosti:

   - ldap://hostname/contextname
   - soubor: [jednotka:] /pathname

   Formát URL LDAP se může lišit v závislosti na poskytovateli LDAP. Další informace naleznete v dokumentaci k protokolu LDAP.

3. Pomocí konfigurace vlastnosti **SECURITY_AUTHENTICATION** definujte, zda rozhraní JNDI předává pověření zabezpečení poskytovateli služeb.

   Tato vlastnost se používá pouze v případě, že je použit poskytovatel služeb LDAP a může mít jednu ze tří hodnot:

   none (anonymní ověření)
   Nastavíte-li tento parametr na hodnotu none, rozhraní JNDI nepředá poskytovateli služeb žádná pověření zabezpečení a provede se *anonymní ověření* .

   simple (jednoduché ověření)
   Nastavíte-li parametr na hodnotu simple, pověření zabezpečení se předají prostřednictvím rozhraní JNDI základnímu poskytovateli služeb. Tato pověření zabezpečení jsou ve formě rozlišujícího jména uživatele (DN uživatele) a hesla.

   CRAM-MD5 (mechanismus ověřováníCRAM-MD5)
   Nastavíte-li parametr na hodnotu CRAM-MD5, pověření zabezpečení se předají prostřednictvím rozhraní JNDI základnímu poskytovateli služeb. Tato pověření zabezpečení jsou ve formě rozlišujícího jména uživatele (DN uživatele) a hesla.

   Pokud nezadáte platnou hodnotu pro vlastnost **SECURITY_AUTHENTICATION** , výchozí hodnota vlastnosti je none.

Jsou-li vyžadována pověření zabezpečení, budete k jejich zadání vyzváni při inicializaci nástroje. Tomu se můžete vyhnout nastavením vlastností **PROVIDER_USERDN** a **PROVIDER_PASSWORD** v konfiguračním souboru JMSAdmin.

Poznámka: Pokud tyto vlastnosti nepoužijete, bude zadaný text *včetně hesla*zobrazen na obrazovce. To může mít bezpečnostní důsledky.

Nástroj sám neprovádí žádné ověření; úloha ověření je delegována na server LDAP. Administrátor serveru LDAP musí nastavit a udržovat přístupová oprávnění k různým částem adresáře. Další informace naleznete v dokumentaci k protokolu LDAP. Pokud ověření selže, nástroj zobrazí odpovídající chybovou zprávu a ukončí se.

Podrobnější informace o zabezpečení a rozhraní JNDI naleznete v dokumentaci na webu Oracle Java (Oracle Technology Network for Java Developers).

Spuštění nástrojů JMSAdmin a JMS30Admin

Nástroje administrace IBM MQ JMS a Jakarta Messaging mají rozhraní příkazového řádku, které můžete použít buď interaktivně, nebo ke spuštění dávkového zpracování.

Informace o této úloze

Interaktivní režim poskytuje příkazový řádek, kde můžete zadat příkazy administrace. V dávkovém režimu příkaz ke spuštění nástroje zahrnuje název souboru, který obsahuje skript příkazu administrace.

Procedura

Interaktivní režim

- Chcete-li spustit nástroj v interaktivním režimu, zadejte následující příkaz:

  JMS 2.0

  ```
  JMSAdmin [-t] [-v] [-cfg config_filename]
  ```

  JM 3.0

  ```
  JMS30Admin [-t] [-v] [-cfg config_filename]
  ```

  kde:

  -t
  Povolí trasování (výchozí nastavení je trasování vypnuto).

  Trasovací soubor je vygenerován v adresáři `"%MQ_JAVA_DATA_PATH%"\errors` (Windows). nebo `/var/mqm/trace` (AIX and Linux). Název trasovacího souboru je ve tvaru:

  `mqjms_`*`PID`*`.trc`

  kde *PID* je ID procesu prostředí JVM.

  -v
  Vytvoří výstup s komentářem (výchozí je výstup s komentářem).

  -cfg název_konfigurace_souboru
  Pojmenuje alternativní konfigurační soubor. Pokud je tento parametr vynechán, použije se výchozí konfigurační soubor `JMSAdmin.config` (pro JMS 2.0) nebo `JMS30Admin.config` (pro Jakarta Messaging 3.0). Další informace o konfiguračním souboru viz téma “Konfigurace nástrojů JMSAdmin a JMS30Admin” na stránce 666.

  Zobrazí se příkazový řádek, který označuje, že nástroj je připraven přijmout příkazy administrace. Tato výzva se na počátku zobrazí jako:

```
InitCtx>
```

Označuje, že aktuální kontext (tj. kontext rozhraní JNDI, na který všechny operace pojmenování a adresáře v současné době odkazují) je počátečním kontextem definovaným v konfiguračním parametru **PROVIDER_URL** . Další informace o tomto parametru naleznete v části “Konfigurace nástrojů JMSAdmin a JMS30Admin” na stránce 666.

Při průchodu adresářovým oborem názvů se výzva k zadání změní tak, aby toto odráželo, takže výzva vždy zobrazuje aktuální kontext.

Dávkový režim

- Chcete-li spustit nástroj v dávkovém režimu, zadejte následující příkaz:

  JMS 2.0

  ```
  JMSAdmin test.scp
  ```

  JM 3.0

  ```
  JMS30Admin test.scp
  ```

  kde *test.scp* je skriptový soubor, který obsahuje příkazy administrace. Další informace viz téma “Použití příkazů administrace s JMSAdmin a JMS30Admin” na stránce 669. Posledním příkazem v souboru musí být příkaz END .

Použití příkazů administrace s JMSAdmin a JMS30Admin

Administrační nástroje produktu IBM MQ JMS a Jakarta Messaging přijímají příkazy sestávající z administračního příkazu a příslušných parametrů.

Informace o této úloze

V následující tabulce jsou uvedena administrační slova, která můžete použít při zadávání příkazů pomocí administračních nástrojů.

Tabulka 37. Administrační slovesa

Sloveso	**Zkrácená forma**	**Popis**
ALTER	ALT	Změnit alespoň jednu z vlastností spravovaného objektu
Definice	DEF	Vytvořit a uložit spravovaný objekt nebo vytvořit dílčí kontext
DISPLAY	DIS	Zobrazit vlastnosti jednoho nebo více uložených spravovaných objektů nebo obsah aktuálního kontextu
ODSTRANIT	DEL	Odeberte jeden nebo více spravovaných objektů z oboru názvů nebo odeberte prázdný dílčí kontext.
CHANGE	chg	Změnit aktuální kontext a umožnit uživateli procházet obor názvů adresáře kdekoli pod počátečním kontextem (nevyřízené zajištění zabezpečení).
COPY	CP	Vytvořit kopii uloženého spravovaného objektu a uložit ji pod alternativním názvem
MOVE	MV	Změnit název, pod kterým je spravovaný objekt uložen
END		Zavřít nástroj pro administraci

Procedura

- Není-li nástroj pro administraci již spuštěn, spusťte jej podle popisu v části “Spuštění nástrojů JMSAdmin a JMS30Admin” na stránce 668.

  Zobrazí se příkazový řádek, který označuje, že nástroj je připraven přijmout příkazy administrace. Tato výzva se na počátku zobrazí jako:

  ```
  InitCtx>
  ```

  Chcete-li změnit aktuální kontext, použijte příkaz CHANGE podle popisu v části “Konfigurace dílčích kontextů” na stránce 670.
- Zadejte příkazy v následujícím formátu:

  ```
  verb [param]*
  ```

  kde **verb** je jedno z administračních příkazových slov uvedených v seznamu Tabulka 37 na stránce 669. Všechny platné příkazy obsahují jedno slovo, které se objeví na začátku příkazu ve standardní nebo zkrácené podobě. Názvy sloves nerozlišují velká a malá písmena.
- Chcete-li ukončit příkaz, stiskněte klávesu Enter, pokud nechcete zadat několik příkazů společně, v takovém případě zadejte znak plus (+) přímo před stisknutím klávesy Enter.

  Chcete-li ukončit příkazy, obvykle stiskněte klávesu Enter. Toto však můžete přepsat zadáním znaménka plus (+) přímo před stisknutím klávesy Enter. To vám umožní zadat víceřádkové příkazy, jak ukazuje následující příklad:

  ```
  DEFINE Q(BookingsInputQueue) +
  QMGR(QM.POLARIS.TEST) +
  QUEUE(BOOKINGS.INPUT.QUEUE) +
  PORT(1415) +
  CCSID(437)
  ```
- Chcete-li zavřít nástroj pro administraci, použijte příkaz **END** .

  Toto slovo nemůže mít žádné parametry.

Konfigurace dílčích kontextů

Pomocí příkazových slov **CHANGE**, **DEFINE**, **DISPLAY** a **DELETE** můžete konfigurovat dílčí kontexty oboru názvů adresáře.

Informace o této úloze

Použití těchto sloves je popsáno v následující tabulce.

Tabulka 38. Syntaxe a popis příkazů používaných k manipulaci s dílčími kontexty

Syntaxe příkazu	**Popis**
DEFINE CTX (ctxName)	Pokusí se vytvořit podřízený dílčí kontext aktuálního kontextu s názvem ctxName. Selže, pokud dojde k narušení zabezpečení, pokud dílčí kontext již existuje, nebo pokud zadaný název není platný.
ZOBRAZENÍ CTX	Zobrazí obsah aktuálního kontextu. Spravované objekty jsou anotovány anotací a, podkontexty anotací [D]. Zobrazí se také typ Java každého objektu.
DELETE CTX (ctxName)	Pokusí se odstranit podřízený kontext aktuálního kontextu s názvem ctxName. Pokud kontext není nalezen, není prázdný nebo došlo k narušení zabezpečení, dojde k selhání.

Tabulka 38. Syntaxe a popis příkazů používaných k manipulaci s dílčími kontexty (pokračování)	
Syntaxe příkazu	**Popis**
CHANGE CTX (ctxName)	Změní aktuální kontext tak, aby nyní odkazoval na podřízený kontext s názvem ctxName. Lze zadat jednu ze dvou speciálních hodnot ctxName : **= SPUŠTĚNO** přesune se na nadřízený prvek aktuálního kontextu **= PROBÍHÁ** přesune se přímo do počátečního kontextu Selže, pokud uvedený kontext neexistuje, nebo pokud dojde k narušení zabezpečení.

Názvy objektů JMS nebo Jakarta Messaging , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jednou z těchto konvencí je, že názvy objektů a kontextů musí obsahovat předponu, například cn= (obecný název) nebo ou= (organizační jednotka). Nástroj pro administraci zjednodušuje používání poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který zadáte. Pro LDAP se jedná o cn=. V případě potřeby můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru. Další informace viz “Konfigurace nástrojů JMSAdmin a JMS30Admin” na stránce 666.

Poznámka: Možná budete muset nakonfigurovat server LDAP tak, aby ukládal objekty Java . Další informace naleznete v dokumentaci k serveru LDAP.

Vytvoření objektů JMS

Chcete-li vytvořit továrnu připojení JMS nebo Jakarta Messaging a cílové objekty a uložit je do oboru názvů JNDI, použijte příkaz DEFINE . Chcete-li ukládat objekty v prostředí LDAP, musíte jim dát názvy, které jsou v souladu s určitými konvencemi. Nástroj pro administraci vám může pomoci dodržovat konvence pojmenování LDAP přidáním výchozí předpony k názvům objektů.

Informace o této úloze

Příkaz DEFINE vytvoří spravovaný objekt s typem, názvem a vlastnostmi, které zadáte. Nový objekt je uložen v aktuálním kontextu.

Názvy objektů JMS nebo Jakarta Messaging , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jednou z těchto konvencí je, že názvy objektů a kontextů musí obsahovat předponu, například cn= (obecný název) nebo ou= (organizační jednotka). Nástroj pro administraci zjednodušuje používání poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který zadáte. Pro LDAP se jedná o cn=. V případě potřeby můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru. Další informace viz “Konfigurace nástrojů JMSAdmin a JMS30Admin” na stránce 666.

Poznámka: Možná budete muset nakonfigurovat server LDAP tak, aby ukládal objekty Java . Další informace naleznete v dokumentaci k serveru LDAP.

Postup

1. Není-li nástroj pro administraci již spuštěn, spusťte jej podle popisu v části “Spuštění nástrojů JMSAdmin a JMS30Admin” na stránce 668.

   Zobrazí se příkazový řádek, který označuje, že nástroj je připraven přijmout příkazy administrace.
2. Ujistěte se, že příkazový řádek zobrazuje kontext, ve kterém chcete vytvořit nový objekt.

   Když spustíte nástroj pro administraci, výzva se na začátku zobrazí jako:

```
InitCtx>
```

Chcete-li změnit aktuální kontext, použijte příkaz CHANGE podle popisu v části “Konfigurace dílčích kontextů” na stránce 670.

3. Chcete-li vytvořit továrnu připojení, cíl fronty nebo cíl tématu, použijte následující syntaxi příkazu:

```
DEFINE TYPE (name) [property]*
```

To znamená, že zadejte příkaz DEFINE následovaný odkazem na spravovaný objekt *TYPE* (name) následovaný žádnými nebo více *vlastnostmi* (viz Vlastnosti IBM MQ classes for JMS objektů).

4. Chcete-li vytvořit továrnu připojení, cíl fronty nebo cíl tématu, použijte následující syntaxi příkazu:

```
DEFINE TYPE (name) [property]*
```

5. Chcete-li zobrazit nově vytvořený objekt, použijte příkaz DISPLAY s následující syntaxí příkazu:

```
DISPLAY TYPE (name)
```

Příklad

Následující příklad ukazuje frontu s názvem testQueue vytvořenou v počátečním kontextu pomocí příkazu DEFINE . Vzhledem k tomu, že se tento objekt ukládá v prostředí LDAP, přestože název objektu `testQueue` není zadán s předponou, nástroj jej automaticky přidá, aby zajistil shodu s konvencí pojmenování LDAP. Zadání příkazu `DISPLAY Q(testQueue)` také způsobí přidání této předpony.

V 9.3.0 JM 3.0 V 9.3.0

```
InitCtx> DEFINE Q(testQueue)

InitCtx> DISPLAY CTX

Contents of InitCtx

a cn=testQueue       com.ibm.mq.jakarta.jms.MQQueue

1 Object(s)
0 Context(s)
1 Binding(s), 1 Administered
```

JMS 2.0

```
InitCtx> DEFINE Q(testQueue)

InitCtx> DISPLAY CTX

Contents of InitCtx

a cn=testQueue       com.ibm.mq.jms.MQQueue

1 Object(s)
0 Context(s)
1 Binding(s), 1 Administered
```

Ukázkové chybové stavy při vytváření objektu JMS

Při vytváření objektu může dojít k řadě běžných chybových stavů.

Zde jsou příklady těchto chybových stavů:

CipherSpec namapovaná na CipherSuite

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SSLCIPHERSUITE(RC4_MD5_US)
WARNING: Converting CipherSpec RC4_MD5_US to
CipherSuite SSL_RSA_WITH_RC4_128_MD5
```

Neplatná vlastnost pro objekt

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PRIORITY(4)
Unable to create a valid object, please check the parameters supplied
Invalid property for a QCF: PRI
```

Neplatný typ pro hodnotu vlastnosti

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) CCSID(english)
Unable to create a valid object, please check the parameters supplied
Invalid value for CCS property: English
```

Kolize vlastností-klient/bindings

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) HOSTNAME(polaris.hursley.ibm.com)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: Client-bindings attribute clash
```

Konflikt vlastností-inicializace ukončení

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SECEXITINIT(initStr)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: ExitInit string supplied
without Exit string
```

Hodnota vlastnosti mimo platný rozsah

```
InitCtx/cn=Trash> DEFINE Q(testQ) PRIORITY(12)
Unable to create a valid object, please check the parameters supplied
Invalid value for PRI property: 12
```

Neznámá vlastnost

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PIZZA(ham and mushroom)
Unable to create a valid object, please check the parameters supplied
Unknown property: PIZZA
```

Zde jsou uvedeny příklady chybových stavů, které mohou nastat v systému Windows při vyhledávání objektů spravovaných rozhraním JNDI z aplikace JMS .

1. Používáte-li poskytovatele rozhraní JNDI WebSphere com.ibm.websphere.naming.WsnInitialContextFactory, musíte použít dopředné lomítko (/) pro přístup ke spravovaným objektům definovaným v dílčích kontextech, například jms/MyQueueName. Pokud použijete zpětné lomítko (\), dojde k výjimce InvalidName.
2. Používáte-li poskytovatele rozhraní JNDI Oracle , com.sun.jndi.fscontext.RefFSContextFactory, musíte pro přístup ke spravovaným objektům definovaným v dílčích kontextech použít zpětné lomítko (\); například ctx1\\fred. Pokud použijete dopředné lomítko (/), dojde k výjimce NameNotFoundException .

Konfigurace objektů JMS

Pomocí příkazových slov ALTER, DEFINE, DISPLAY, DELETE, COPYa MOVE můžete manipulovat se spravovanými objekty v oboru názvů adresáře.

Informace o této úloze

Tabulka 39 na stránce 674 shrnuje použití těchto sloves. Řetězec *TYPE* nahraďte klíčovým slovem, které představuje požadovaný spravovaný objekt, jak je popsáno v tématu “Konfigurace objektů JMS a Jakarta Messaging pomocí nástrojů pro administraci” na stránce 664.

Tabulka 39. Syntaxe a popis příkazů používaných pro manipulaci se spravovanými objekty	
Syntaxe příkazu	**Popis**
ALTER *TYPE* (název) [vlastnost] *	Pokusí se aktualizovat vlastnosti spravovaného objektu pomocí zadaných vlastností. Selže, pokud dojde k narušení zabezpečení, pokud uvedený objekt nelze nalézt, nebo pokud zadané nové vlastnosti nejsou platné.
DEFINE *TYPE* (name) [property] *	Pokusí se vytvořit spravovaný objekt typu *TYPE* s dodanými vlastnostmi a uložit jej pod názvem name v aktuálním kontextu. Pokud dojde k narušení zabezpečení, pokud zadaný název není platný nebo objekt s tímto názvem existuje nebo pokud zadané vlastnosti nejsou platné, dojde k selhání.
DISPLAY *TYPE* (název)	Zobrazí vlastnosti spravovaného objektu typu *TYPE* , svázaného pod názvem name v aktuálním kontextu. Pokud objekt neexistuje nebo došlo k narušení zabezpečení, dojde k selhání.
DELETE *TYPE* (název)	Pokusí se odebrat spravovaný objekt typu *TYPE* s názvem namez aktuálního kontextu. Pokud objekt neexistuje nebo došlo k narušení zabezpečení, dojde k selhání.
KOPIE *TYPE* (nameA) *TYPE* (nameB)	Vytvoří kopii spravovaného objektu typu *TYPE* s názvem nameAa pojmenováním kopie nameB. Toto vše se vyskytuje v rámci rozsahu aktuálního kontextu. Selže, pokud objekt, který se má zkopírovat, neexistuje, pokud existuje objekt s názvem nameB nebo pokud došlo k narušení zabezpečení.
MOVE *TYPE* (nameA) *TYPE* (nameB)	Přesune (přejmenuje) spravovaný objekt typu *TYPE* s názvem nameAdo adresáře nameB. Toto vše se vyskytuje v rámci rozsahu aktuálního kontextu. Pokud objekt, který má být přesunut, neexistuje, pokud existuje objekt s názvem nameB nebo pokud došlo k narušení zabezpečení, dojde k selhání.

JMS 2.0 Konfigurace prostředků JMS 2.0 v adresáři WebSphere Application Server

Chcete-li nakonfigurovat prostředky JMS 2.0 v produktu WebSphere Application Server, můžete použít buď administrativní konzolu, nebo příkazy wsadmin.

Než začnete

V 9.3.0 JM 3.0 V 9.3.0 Ačkoli IBM MQ 9.3 podporuje Jakarta Messaging 3.0, WebSphere Application Server momentálně nemá ekvivalentní podporu. Proto v produktu WebSphere Application Serverkonfigurujete prostředky Java Message Service 2.0 .

Informace o této úloze

Aplikace Java Message Service 2.0 obvykle spoléhají na externě nakonfigurované objekty, které popisují, jak se aplikace připojuje ke svému poskytovateli produktu JMS a k cílům, ke kterým přistupuje. Aplikace JMS používají funkci Java Naming Directory Interface (JNDI) pro přístup k následujícím typům objektů za běhu:

- Specifikace aktivace (používané aplikačními servery Java EE)
- Unifikované továrny připojení (s produktem JMS 1.1 a novějšími továrnami připojení, které jsou nezávislé na doméně (unifikované), jsou upřednostňovány před továrnami připojení front a továrnami připojení témat specifických pro doménu).

- Továrny připojení tématu (používané aplikacemi JMS 1.0)
- Továrny připojení fronty (používané aplikacemi JMS 1.0)
- Fronty
- Témata

Prostřednictvím poskytovatele systému zpráv IBM MQ v produktu WebSphere Application Servermohou aplikace systému zpráv Java Message Service (JMS) používat systém IBM MQ jako externího poskytovatele prostředků systému zpráv JMS . Chcete-li tento přístup povolit, konfigurujte poskytovatele systému zpráv IBM MQ v adresáři WebSphere Application Server tak, aby definoval prostředky JMS pro připojení k libovolnému správci front v síti IBM MQ .

Produkt WebSphere Application Server můžete použít ke konfiguraci prostředků IBM MQ pro aplikace (například továrny připojení fronty) a ke správě zpráv a odběrů přidružených k místům určení JMS . Zabezpečení spravujete prostřednictvím produktu IBM MQ.

Související úlohy

Společné použití IBM MQ a WebSphere Application Server

WebSphere Application Server Témata

Spolupráce s poskytovatelem systému zpráv IBM MQ

Správa systému zpráv s poskytovatelem systému zpráv IBM MQ

Mapování názvů panelů administrativní konzoly na názvy příkazů a názvy IBM MQ

JMS 2.0 Konfigurace prostředků JMS 2.0 pomocí administrativní konzoly

Prostřednictvím administrativní konzoly produktu WebSphere Application Server můžete konfigurovat specifikace aktivace, továrny připojení a místa určení pro poskytovatele produktu IBM MQ JMS .

Informace o této úloze

Administrativní konzolu WebSphere Application Server můžete použít k vytvoření, zobrazení nebo úpravě libovolného z následujících prostředků:

- Specifikace aktivace
- Továrny připojení nezávislé na doméně (JMS 1.1 nebo novější)
- Továrny připojení fronty
- Továrny připojení tématu
- Fronty
- Témata

Následující kroky poskytují přehled způsobů, jak můžete použít administrativní konzolu ke konfiguraci prostředků JMS pro použití s poskytovatelem systému zpráv IBM MQ . Každý krok obsahuje název tématu v dokumentaci k produktu WebSphere Application Server , na který se můžete odkázat, abyste získali další informace. Odkazy na tato témata v části IBM Documentationviz *Související odkazy* .

V buňce WebSphere Application Server se smíšenými verzemi můžete spravovat prostředky produktu IBM MQ v uzlech všech verzí. Některé vlastnosti však nejsou k dispozici ve všech verzích. V této situaci se v administrativní konzole zobrazí pouze vlastnosti konkrétního uzlu.

Procedura

Chcete-li vytvořit nebo konfigurovat specifikaci aktivace pro použití s poskytovatelem systému zpráv IBM MQ , postupujte takto:

- Chcete-li vytvořit specifikaci aktivace, použijte průvodce Vytvořit prostředek IBM MQ JMS .

  Buď můžete pomocí průvodce určit všechny podrobnosti pro specifikaci aktivace, nebo můžete určit podrobnosti připojení pro produkt IBM MQ pomocí tabulky CCDT (Client Channel Definition Table). Při zadávání podrobností o připojení pomocí průvodce můžete buď zadat informace o hostiteli a portu samostatně, nebo, používáte-li správce front s více instancemi, zadat informace o hostiteli a portu ve

formě seznamu názvů připojení. Další informace naleznete v tématu *Vytvoření specifikace aktivace pro IBM MQ poskytovatele systému zpráv*.

- Chcete-li zobrazit nebo změnit vlastnosti konfigurace specifikace aktivace, použijte panel nastavení továrny připojení poskytovatele systému zpráv IBM MQ administrativní konzoly.

  Tyto konfigurační vlastnosti řídí způsob vytváření připojení k přidruženým frontám a tématům. Další informace naleznete v tématu *Konfigurace specifikace aktivace pro IBM MQ poskytovatele systému zpráv*.

Chcete-li vytvořit nebo konfigurovat unifikovanou továrnu připojení, továrnu připojení fronty nebo továrnu připojení tématu pro použití s poskytovatelem systému zpráv IBM MQ , postupujte takto:

- Chcete-li vytvořit továrnu připojení, nejprve vyberte typ továrny připojení, kterou chcete vytvořit, a poté pomocí průvodce vytvořením prostředku IBM MQ JMS zadejte podrobnosti.
  - Pokud má vaše aplikace JMS používat pouze systém zpráv typu point-to-point, vytvořte pro doménu systému zpráv typu point-to-point továrnu připojení specifickou pro doménu systému zpráv typu point-to-point, kterou lze použít pro vytváření připojení specificky pro systém zpráv typu point-to-point.
  - Pokud má vaše aplikace JMS používat pouze systém zpráv publikování/odběru, vytvořte pro doménu systému zpráv publikování/odběru továrnu připojení specifickou pro doménu systému zpráv publikování/odběru, kterou lze použít pro vytváření připojení specificky pro systém zpráv publikování/odběru.
  - Pro systém JMS 1.1 nebo novější vytvořte továrnu připojení nezávislou na doméně, kterou lze použít pro systém zpráv typu point-to-point i pro systém zpráv publikování/odběru, což vaší aplikaci umožní provádět práci typu point-to-point i publikování/odběr v rámci stejné transakce.

  Můžete zvolit, zda chcete použít průvodce k určení všech podrobností pro továrnu připojení, nebo zda chcete určit podrobnosti připojení pro produkt IBM MQ pomocí tabulky CCDT (Client Channel Definition Table). Při zadávání podrobností o připojení pomocí průvodce můžete buď zadat informace o hostiteli a portu samostatně, nebo, používáte-li správce front s více instancemi, zadat informace o hostiteli a portu ve formě seznamu názvů připojení. Další informace naleznete v tématu *Vytvoření továrny připojení pro IBM MQ poskytovatele systému zpráv*.

Chcete-li zobrazit nebo změnit vlastnosti konfigurace továrny připojení, postupujte takto:

- Použijte panel nastavení továrny připojení administrativní konzoly pro typ továrny připojení, kterou chcete konfigurovat.

  Vlastnosti konfigurace řídí způsob vytváření připojení k přidruženým frontám a tématům. Další informace naleznete v tématu *Konfigurace továrny kolekce pro IBM MQ poskytovatele systému zpráv*nebo *Konfigurace továrny kolekce front pro IBM MQ poskytovatele systému zpráv*nebo *Konfigurace továrny kolekce témat pro IBM MQ poskytovatele systému zpráv*.

Chcete-li konfigurovat cíl fronty JMS pro dvoubodový systém zpráv s poskytovatelem systému zpráv IBM MQ , postupujte takto:

- Prostřednictvím panelu nastavení fronty poskytovatele systému zpráv IBM MQ administrativní konzoly můžete definovat následující typy vlastností:
  - Obecné vlastnosti, včetně vlastností administrace a fronty IBM MQ .
  - Vlastnosti připojení, které určují způsob připojení ke správci front, který je hostitelem fronty.
  - Rozšířené vlastnosti, které řídí chování připojení k místům určení poskytovatele systému zpráv IBM MQ .
  - Všechny přizpůsobené vlastnosti pro cíl fronty.

  Další informace naleznete v tématu *Konfigurace fronty pro IBM MQ poskytovatele systému zpráv*.

Chcete-li vytvořit nebo konfigurovat místo určení tématu JMS pro systém zpráv publikování/odběru s poskytovatelem systému zpráv IBM MQ , postupujte takto:

- Na panelu nastavení tématu poskytovatele systému zpráv IBM MQ můžete definovat následující typy vlastností:
  - Obecné vlastnosti včetně vlastností administrace a tématu IBM MQ .

- Rozšířené vlastnosti, které řídí chování připojení k místům určení poskytovatele systému zpráv IBM MQ .
- Všechny přizpůsobené vlastnosti pro cíl fronty.

Další informace naleznete v tématu *Konfigurace tématu pro IBM MQ poskytovatele systému zpráv*.

Související pojmy

“Správci front s více instancemi” na stránce 493
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 rezervní instance. Pokud se aktivní instance nezdaří, správce front pro více instancí se automaticky restartuje na záložním serveru.

Související úlohy

“Konfigurace binárního formátu CCDT” na stránce 41
Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformě Multiplatforms se při vytvoření správce front automaticky vytvoří binární tabulka CCDT obsahující výchozí nastavení. Příkaz **runmqsc** se používá k aktualizaci binární tabulky CCDT.

“Konfigurace publikování/odběru zpráv” na stránce 421
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.

WebSphere Application Server Témata

Specifikace aktivace poskytovatele systému zpráv IBM MQ
Vytvoření specifikace aktivace pro poskytovatele systému zpráv IBM MQ
Konfigurace specifikace aktivace pro poskytovatele systému zpráv IBM MQ
Vytvoření továrny připojení pro poskytovatele systému zpráv IBM MQ
Konfigurace unifikované továrny připojení pro poskytovatele systému zpráv IBM MQ
Konfigurace továrny připojení fronty pro poskytovatele systému zpráv IBM MQ
Konfigurace továrny připojení tématu pro poskytovatele systému zpráv IBM MQ
Konfigurace fronty pro poskytovatele systému zpráv IBM MQ
Konfigurace tématu pro poskytovatele systému zpráv IBM MQ

JMS 2.0 Konfigurace prostředků JMS 2.0 pomocí skriptovacích příkazů wsadmin

Skriptovací příkazy WebSphere Application Server wsadmin můžete použít k vytvoření, úpravě, odstranění nebo zobrazení informací o specifikacích aktivace JMS , továrnách připojení, frontách a tématech. Můžete také zobrazit a spravovat nastavení pro adaptér prostředků IBM MQ .

Informace o této úloze

Následující kroky poskytují přehled způsobů použití příkazů WebSphere Application Server wsadmin ke konfiguraci prostředků JMS pro použití s poskytovatelem systému zpráv IBM MQ . Další informace o použití těchto příkazů naleznete v tématu *Související odkazy* , které obsahuje odkazy na dokumentaci k produktu WebSphere Application Server .

Chcete-li spustit příkaz, použijte objekt AdminTask skriptovacího klienta wsadmin.

Po použití příkazu k vytvoření nového objektu nebo provedení změn uložte změny do hlavní konfigurace. Použijte například následující příkaz:

```
AdminConfig.save()
```

Chcete-li zobrazit seznam dostupných administrativních příkazů poskytovatele systému zpráv IBM MQ a jejich stručný popis, zadejte na příkazový řádek nástroje wsadmin následující příkaz:

```
print AdminTask.help('WMQAdminCommands')
```

Chcete-li zobrazit přehledovou nápovědu k danému příkazu, zadejte na příkazový řádek nástroje wsadmin následující příkaz:

```
print AdminTask.help('command_name')
```

Procedura

Chcete-li vypsat všechny prostředky poskytovatele systému zpráv IBM MQ definované v oboru, ve kterém je příkaz vydán, použijte následující příkazy.

- Chcete-li vypsat specifikace aktivace, použijte příkaz **listWMQActivationSpecs** .
- Chcete-li vypsat továrny připojení, použijte příkaz **listWMQConnectionFactories** .
- Chcete-li vypsat cíle typu fronty, použijte příkaz **listWMQQueues** .
- Chcete-li vypsat místa určení typu tématu, použijte příkaz **listWMQTopics** .

Chcete-li vytvořit prostředek JMS pro poskytovatele systému zpráv IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li vytvořit specifikaci aktivace, použijte příkaz **createWMQActivationSpec** .

  Můžete buď vytvořit specifikaci aktivace zadáním všech parametrů, které mají být použity pro vytvoření připojení, nebo můžete vytvořit specifikaci aktivace tak, aby k vyhledání správce front pro připojení používala tabulku CCDT (Client Channel Definition Table).
- Chcete-li vytvořit továrnu připojení, použijte příkaz **createWMQConnectionFactory** s parametrem **-type** a určete typ továrny připojení, kterou chcete vytvořit:
  - Pokud má vaše aplikace JMS používat pouze systém zpráv typu point-to-point, vytvořte pro doménu systému zpráv typu point-to-point továrnu připojení specifickou pro doménu systému zpráv typu point-to-point, kterou lze použít pro vytváření připojení specificky pro systém zpráv typu point-to-point.
  - Pokud má vaše aplikace JMS používat pouze systém zpráv publikování/odběru, vytvořte pro doménu systému zpráv publikování/odběru továrnu připojení specifickou pro doménu systému zpráv publikování/odběru, kterou lze použít pro vytváření připojení specificky pro systém zpráv publikování/odběru.
  - Pro systém JMS 1.1 nebo novější vytvořte továrnu připojení nezávislou na doméně, kterou lze použít pro systém zpráv typu point-to-point i pro systém zpráv publikování/odběru, což vaší aplikaci umožní provádět práci typu point-to-point i publikování/odběr v rámci stejné transakce.

  Výchozí typ je továrna připojení nezávislá na doméně.
- Chcete-li vytvořit cíl typu fronty, použijte příkaz **createWMQQueue** .
- Chcete-li vytvořit místo určení typu tématu, použijte příkaz **createWMQTopic** .

Chcete-li upravit prostředek JMS pro poskytovatele systému zpráv IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li upravit specifikaci aktivace, použijte příkaz **modifyWMQActivationSpec** .

  Typ specifikace aktivace nelze změnit. Například nemůžete vytvořit specifikaci aktivace, kde zadáte všechny informace o konfiguraci ručně a pak ji upravíte tak, aby používala CCDT.
- Chcete-li upravit továrnu připojení, použijte příkaz **modifyWMQConnectionFactory** .
- Chcete-li upravit místo určení typu fronty, použijte příkaz **modifyWMQQueue** .
- Chcete-li upravit místo určení typu tématu, použijte příkaz **modifyWMQTopic** .

Chcete-li odstranit prostředek JMS pro poskytovatele systému zpráv IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li odstranit specifikaci aktivace, použijte příkaz **deleteWMQActivationSpec** .
- Chcete-li odstranit továrnu na připojení, použijte příkaz **deleteWMQConnectionFactory** .
- Chcete-li odstranit cíl typu fronty, použijte příkaz **deleteWMQQueue** .
- Chcete-li odstranit místo určení typu tématu, použijte příkaz **deleteWMQTopic** .

Chcete-li zobrazit informace o specifickém prostředku poskytovatele systému zpráv IBM MQ , použijte následující příkazy.

- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené ke konkrétní specifikaci aktivace, použijte příkaz **showWMQActivationSpec** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené ke konkrétní továrně připojení, použijte příkaz **showWMQConnectionFactory** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené ke konkrétnímu cíli typu fronty, použijte příkaz **showWMQQueue** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k místu určení typu tématu, použijte příkaz **deleteWMQTopic** .

Chcete-li spravovat nastavení pro adaptér prostředků IBM MQ nebo poskytovatele systému zpráv IBM MQ , použijte následující příkazy.

- Chcete-li spravovat nastavení adaptéru prostředků IBM MQ , který je instalován v určitém oboru, použijte příkaz **manageWMQ** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty, které lze nastavit pomocí příkazu **manageWMQ** , použijte příkaz **showWMQ** . Tato nastavení souvisejí buď s adaptérem prostředků IBM MQ , nebo s poskytovatelem systému zpráv IBM MQ . Příkaz **showWMQ** také zobrazí všechny přizpůsobené vlastnosti, které jsou nastaveny na adaptéru prostředků IBM MQ .

Související pojmy

“Správci front s více instancemi” na stránce 493
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 rezervní instance. Pokud se aktivní instance nezdaří, správce front pro více instancí se automaticky restartuje na záložním serveru.

Související úlohy

“Konfigurace binárního formátu CCDT” na stránce 41
Tabulka CCDT (Client Channel Definition Table) určuje definice kanálů a informace o ověřování používané klientskými aplikacemi pro připojení ke správci front. Na platformě Multiplatforms se při vytvoření správce front automaticky vytvoří binární tabulka CCDT obsahující výchozí nastavení. Příkaz **runmqsc** se používá k aktualizaci binární tabulky CCDT.

“Konfigurace publikování/odběru zpráv” na stránce 421
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.

WebSphere Application Server Témata

createWMQActivationSpec příkaz
createWMQConnectionFactory příkaz
createWMQQueue příkaz
createWMQTopic příkaz
deleteWMQActivationSpec příkaz
deleteWMQConnectionFactory příkaz
deleteWMQQueue příkaz
deleteWMQTopic příkaz
listWMQActivationSpecs příkaz
listWMQConnectionFactories příkaz
listWMQQueues příkaz
listWMQTopics příkaz

modifyWMQActivationSpec příkaz
modifyWMQConnectionFactory příkaz
modifyWMQQueue příkaz
modifyWMQTopic příkaz
showWMQActivationSpec příkaz
showWMQConnectionFactory příkaz
showWMQQueue příkaz
showWMQTopic příkaz
showWMQ příkaz
manageWMQ příkaz

JMS 2.0 Použití sdílených odběrů JMS 2.0

V produktu WebSphere Application Server traditional 9.0můžete konfigurovat a používat JMS 2.0 sdílené odběry s produktem IBM MQ 9.0.

Informace o této úloze

Specifikace JMS 2.0 zavedla koncept sdílených odběrů, který umožňuje otevření jednoho nebo více odběratelů. Zprávy jsou sdíleny mezi všemi těmito spotřebiteli. Neexistuje žádné omezení, pokud se tito spotřebitelé připojují ke stejnému správci front.

Sdílené odběry mohou být buď trvalé, nebo netrvalé, se stejnou sémantikou jako nyní označované jako nesdílené odběry.

Aby mohl spotřebitel identifikovat, který odběr má použít, musí zadat název odběru. Toto je podobné nesdíleným trvalým odběrům, ale ve všech případech, kdy je vyžadován sdílený odběr, je vyžadován název odběru. clientIDvšak není vyžadováno v případě trvalého sdíleného odběru; lze jej zadat, ale není povinný.

Zatímco sdílené odběry lze považovat za mechanizmus vyrovnávání zátěže, ve specifikaci IBM MQ ani JMS 2.0 není žádný závazek týkající se způsobu, jakým jsou zprávy distribuovány mezi spotřebiteli.

V produktu WebSphere Application Server traditional 9.0 je předinstalován adaptér prostředků IBM MQ 9.0 .

Následující kroky ukazují, jak nakonfigurovat specifikaci aktivace tak, aby používala sdílený trvalý nebo sdílený trvalý odběr pomocí administrativní konzoly produktu WebSphere Application Server traditional .

Postup

Nejprve vytvořte objekty v adresáři JNDI.

1. Vytvořte místo určení tématu v adresáři JNDI jako normální (viz “Konfigurace prostředků JMS 2.0 pomocí administrativní konzoly” na stránce 675).
2. Vytvořte specifikaci aktivace (viz “Konfigurace prostředků JMS 2.0 pomocí administrativní konzoly” na stránce 675).

   Specifikaci aktivace můžete vytvořit přesně s vlastnostmi, které potřebujete. Chcete-li použít trvalý odběr, můžete jej vybrat při vytvoření a zadat název. Chcete-li použít netrvalý odběr, nelze v tomto bodě zadat název. Namísto toho je třeba vytvořit přizpůsobenou vlastnost pro název odběru.

Aktualizujte specifikaci aktivace, kterou jste vytvořili, pomocí požadovaných přizpůsobených vlastností. Existují dvě přizpůsobené vlastnosti, které může být nutné zadat:

- Ve všech případech musíte vytvořit přizpůsobenou vlastnost, která určí, že tato specifikace aktivace by měla používat sdílený odběr.
- Pokud byl odběr vytvořen jako netrvalý, vlastnost názvu odběru musí být nastavena jako přizpůsobená vlastnost.

V následující tabulce jsou uvedeny platné hodnoty, které můžete zadat pro každou přizpůsobenou vlastnost:

Název vlastnosti	Typ	Platné hodnoty
sharedSubscription	Řetězec	true, false
subscriptionName	Řetězec	Nenulová délka řetězce java

3. Vyberte specifikaci aktivace ze seznamu zobrazeného ve formuláři **Kolekce specifikací aktivace** .

   Podrobnosti pro specifikaci aktivace jsou zobrazeny ve formuláři **IBM MQ Nastavení specifikace aktivace poskytovatele systému zpráv** .
4. Ve formuláři **IBM MQ nastavení specifikace aktivace poskytovatele systému zpráv** klepněte na volbu **Přizpůsobené vlastnosti**.

   Zobrazí se formulář **Přizpůsobené vlastnosti** .
5. Používáte-li netrvalý odběr, vytvořte přizpůsobenou vlastnost subscriptionName .

   Na panelu **Přizpůsobené vlastnosti** specifikace aktivace klepněte na volbu **Nový**a zadejte následující podrobnosti:

   Název

   Název přizpůsobené vlastnosti, která je v tomto případě `subscriptionName`.

   Hodnota

   Hodnota pro přizpůsobenou vlastnost. Můžete použít názvy JNDI v poli **Hodnota** , například `WASSharedSub0ne`.

   Typ

   Typ přizpůsobené vlastnosti. Vyberte typ přizpůsobené vlastnosti ze seznamu, který v tomto případě musí být `java.lang.String`.
6. Pro sdílený trvalý i sdílený netrvalý odběr vytvořte přizpůsobenou vlastnost sharedSubscription .

   Na panelu **Přizpůsobené vlastnosti** specifikace aktivace klepněte na volbu **Nový**a zadejte následující podrobnosti:

   Název

   Název přizpůsobené vlastnosti, která je v tomto případě `sharedSubscription`.

   Hodnota

   Hodnota pro přizpůsobenou vlastnost. Chcete-li určit, že specifikace aktivace používá sdílený odběr, nastavte hodnotu na `true`. Chcete-li později ukončit používání sdíleného odběru pro tuto specifikaci aktivace, můžete tak učinit nastavením této přizpůsobené vlastnosti na hodnotu `false`.

   Typ

   Typ přizpůsobené vlastnosti. Vyberte typ přizpůsobené vlastnosti ze seznamu, který v tomto případě musí být `java.lang.String`.
7. Po nastavení vlastností restartujte aplikační server.

   Objekty typu message-driven bean (MDB) pro specifikace aktivace jsou poté řízeny při doručení zpráv, ale pouze objekty MDB sdílejí odeslané zprávy.

Související pojmy

Klonované a sdílené odběry

Trvanlivost předplatného

Související úlohy

Konfigurace adaptéru prostředků pro příchozí komunikaci

Související informace pro WebSphere Application Server traditional 9.0

Konfigurace tématu pro poskytovatele systému zpráv IBM MQ

Specifikace aktivace poskytovatele systému zpráv IBM MQ

Vytvoření specifikace aktivace pro poskytovatele systému zpráv IBM MQ

Konfigurace specifikace aktivace pro poskytovatele systému zpráv IBM MQ

JMS 2.0 Použití vlastností JMS 2.0 ConnectionFactory a Destination Lookup

V produktu WebSphere Application Server traditional 9.0mohou být vlastnosti ConnectionFactoryLookup a DestinationLookup specifikace aktivace poskytnuty s názvem JNDI spravovaného objektu, který má být použit jako předvolba k ostatním vlastnostem specifikace aktivace.

Informace o této úloze

Specifikace JMS 2.0 určuje dvě další vlastnosti specifikace aktivace používané k řízení objektů typu message-driven bean (MDB). Dříve musel každý dodavatel zadat přizpůsobené vlastnosti ve specifikaci aktivace, aby poskytoval podrobnosti, které jsou nezbytné pro připojení k systému zpráv, a aby definoval, ze kterého místa určení mají být zprávy získávány.

Nyní standardní vlastnosti connectionFactoryLookup a destinationLookup lze použít k zadání názvu JNDI příslušného objektu, který se má vyhledat a použít. V produktu WebSphere Application Server traditional 9.0 je předinstalován adaptér prostředků IBM MQ 9.0 .

Následující postup ukazuje, jak upravit a použít tyto dvě vlastnosti pomocí administrativní konzoly WebSphere Application Server traditional .

Postup

Nejprve vytvořte objekty v adresáři JNDI.

1. Vytvořte ConnectionFactory v souboru JNDI jako normální (viz “Konfigurace prostředků JMS 2.0 pomocí administrativní konzoly” na stránce 675).
2. Vytvořte cíl v souboru JNDI jako normální (viz “Konfigurace prostředků JMS 2.0 pomocí administrativní konzoly” na stránce 675).

   Cílový objekt musí mít správné hodnoty.
3. Vytvořte specifikaci aktivace s použitím všech potřebných hodnot (viz “Konfigurace prostředků JMS 2.0 pomocí administrativní konzoly” na stránce 675).

   Specifikaci aktivace můžete vytvořit přesně s vlastnostmi, které potřebujete. Měli byste však mít na paměti následující aspekty:

   - Chcete-li, aby adaptér prostředků IBM MQ používal vlastnosti vyhledávání továrny připojení a místa určení produktu Java EE , je méně důležité, jaké vlastnosti se používají při vytváření specifikace aktivace (viz ActivationSpec ConnectionFactoryVlastnosti vyhledání a DestinationLookup.
   - V rámci specifikace aktivace však musí být určena jakákoli vlastnost, která dosud není definována v továrně připojení nebo v místě určení. Proto musíte definovat vlastnosti spotřebitele připojení a další vlastnosti a ověřovací informace, které se použijí při skutečném vytvoření připojení.
   - Z vlastností definovaných v továrně připojení má vlastnost ClientID speciální zpracování. Důvodem je, že běžný scénář používá jednu továrnu na připojení s více specifikacemi aktivace. To zjednodušuje administraci, avšak specifikace JMS vyžaduje jedinečná ID klienta, a proto musí mít specifikace aktivace možnost přepsat jakoukoli hodnotu nastavenou v ConnectionFactory. Není-li pro specifikaci aktivace nastavena žádná hodnota ClientID , bude použita libovolná hodnota pro továrnu připojení.

Buď aktualizujte specifikaci aktivace, kterou jste vytvořili, pomocí dvou nových přizpůsobených vlastností pomocí administrativní konzoly WebSphere Application Server , jak je popsáno v kroku “4” na stránce 682, nebo použijte anotace, jak je popsáno v kroku “5” na stránce 683.

4. Aktualizujte specifikaci aktivace v administrativní konzole WebSphere Application Server .

   Tyto dvě vlastnosti je třeba nastavit na panelu přizpůsobených vlastností specifikace aktivace. Tyto vlastnosti nejsou přítomny na hlavních panelech specifikace aktivace ani v průvodci vytvořením specifikace aktivace.

   a) Vyberte specifikaci aktivace ze seznamu zobrazeného ve formuláři **Kolekce specifikací aktivace** .

      Podrobnosti pro specifikaci aktivace jsou zobrazeny ve formuláři **IBM MQ Nastavení specifikace aktivace poskytovatele systému zpráv** .

b) Ve formuláři **IBM MQ nastavení specifikace aktivace poskytovatele systému zpráv** klepněte na volbu **Přizpůsobené vlastnosti**.

Zobrazí se formulář **Přizpůsobené vlastnosti** .

c) Ve formuláři **Přizpůsobené vlastnosti** vytvořte dvě nové přizpůsobené vlastnosti, obě typu java.lang.String.

V každém případě klepněte na volbu **Nový** a poté zadejte pro přizpůsobenou vlastnost následující podrobnosti:

Název

Název přizpůsobené vlastnosti, buď `connectionFactoryLookup` , nebo `destinationLookup`.

Hodnota

Hodnota pro přizpůsobenou vlastnost. Můžete použít názvy JNDI v poli **Hodnota** , například `QuoteCF` a `QuoteQ`.

Typ

Typ přizpůsobené vlastnosti. Vyberte typ přizpůsobené vlastnosti ze seznamu, který v tomto případě musí být `java.lang.String`.

Implementovaný objekt MDB nyní použije tyto hodnoty k vytvoření továrny připojení a cíle. Při implementaci objektu typu message-driven bean není nutné nastavovat konfiguraci hodnoty JNDI .

5. Místo specifikace aktivace použijte anotace.

K určení hodnot je možné použít anotace v kódu MDB. Například pomocí JNDI names `QuoteCF` a `QuoteQ`by tento kód vypadal takto:

```
@MessageDriven(activationConfig = {
        @ActivationConfigProperty(propertyName =  "destinationType" , propertyValue =
"javax.jms.Topic" ),
        @ActivationConfigProperty(propertyName =  "destinationLookup" , propertyValue =
"QuoteQ" ),
        @ActivationConfigProperty(propertyName =  "connectionFactoryLookup" , propertyValue
=  "QuoteCF" )}, mappedName =  "LookupMDB" )
        @TransactionAttribute(TransactionAttributeType.REQUIRED)
        @TransactionManagement(TransactionManagementType.CONTAINER)
        publicclass LookupMDB implements MessageListener {
```

Související úlohy

Konfigurace adaptéru prostředků pro příchozí komunikaci

Související informace pro WebSphere Application Server traditional 9.0

Konfigurace unifikované továrny připojení pro poskytovatele systému zpráv IBM MQ

Konfigurace tématu pro poskytovatele systému zpráv IBM MQ

Specifikace aktivace poskytovatele systému zpráv IBM MQ

Vytvoření specifikace aktivace pro poskytovatele systému zpráv IBM MQ

Konfigurace specifikace aktivace pro poskytovatele systému zpráv IBM MQ

Konfigurace přizpůsobených vlastností pro prostředky IBM MQ poskytovatele systému zpráv JMS

Konfigurace produktu WebSphere Application Server pro použití nejnovější úrovně údržby adaptéru prostředků

Chcete-li zajistit automatickou aktualizaci adaptéru prostředků IBM MQ na nejnovější dostupnou úroveň údržby při použití opravných sad WebSphere Application Server , můžete nakonfigurovat všechny servery ve vašem prostředí tak, aby používaly nejnovější verzi adaptéru prostředků obsaženou v opravné sadě WebSphere Application Server , kterou jste použili pro instalaci jednotlivých uzlů.

Než začnete

Důležité:

- JMS 3.0 WebSphere Application Server traditional v současné době nepodporuje Jakarta EE. Viz IBM MQ prohlášení o podpoře adaptéru prostředků.
- Používáte-li produkt WebSphere Application Server 8.5 nebo starší na libovolné platformě, neinstalujte adaptér prostředků IBM MQ 8.0 nebo novější na aplikační server. Adaptér prostředků IBM MQ 8.0 nebo novější lze implementovat pouze na aplikační server, který podporuje produkt JMS 2.0. Produkt WebSphere Application Server 8.5 nebo starší však podporuje pouze produkt JMS 1.1.

Informace o této úloze

Tuto úlohu použijte, pokud se na vaši konfiguraci vztahují některé z následujících okolností a chcete nakonfigurovat všechny servery ve vašem prostředí tak, aby používaly nejnovější verzi adaptéru prostředků IBM MQ :

- Protokoly prostředí JVM libovolného aplikačního serveru ve vašem prostředí zobrazují následující informace o verzi adaptéru prostředků IBM MQ po použití produktu WebSphere Application Server 7.0.0 Fix Pack 1 nebo novějšího:

  ```
  WMSG1703I:RAR verze implementace 7.0.0.0-k700-L080820
  ```

- Protokoly JVM libovolného aplikačního serveru ve vašem prostředí obsahují následující položku:

  ```
  WMSG1625E: Nebylo možné zjistit
  kód poskytovatele systému zpráv IBM MQ v zadané cestě < null>
  ```

- Jeden nebo více uzlů bylo dříve ručně aktualizováno, aby používalo specifickou úroveň údržby adaptéru prostředků IBM MQ , která je nyní nahrazena nejnovější verzí adaptéru prostředků obsaženého v aktuální úrovni údržby produktu WebSphere Application Server .

Adresář *profile_root* , na který příklady odkazují, je domovským adresářem profilu WebSphere Application Server , například `C:\Program Files\IBM\WebSphere\AppServer1`.

Po provedení následujících kroků pro všechny buňky a instalace s jedním serverem ve vašem prostředí vaše servery automaticky obdrží údržbu adaptéru prostředků IBM MQ při použití nové opravné sady WebSphere Application Server .

Postup

1. Spusťte aplikační server. Pokud je profil součástí konfigurace síťové implementace, spusťte správce implementace a všechny agenty uzlů. Pokud profil obsahuje administrativního agenta, spusťte administrativního agenta.
2. Zkontrolujte úroveň údržby adaptéru prostředků IBM MQ .
   a) Otevřete okno příkazového řádku a přejděte do adresáře *profile_root*`\bin` .

      Zadejte například `cd C:\Program Files\IBM\WebSphere\AppServer1\bin`.

   b) Spusťte nástroj wsadmin tak, že zadáte `wsadmin.bat -lang jython`, a pokud k tomu budete vyzváni, zadejte své jméno uživatele a heslo.

   c) Zadejte následující příkaz a dvakrát stiskněte klávesu Return:

```
wmqInfoMBeansUnsplit = AdminControl.queryNames("WebSphere:type=WMQInfo,*")
wmqInfoMBeansSplit = AdminUtilities.convertToList(wmqInfoMBeansUnsplit)
for wmqInfoMBean in wmqInfoMBeansSplit: print wmqInfoMBean; print AdminControl.invoke(wmqInfoMBean,
'getInfo', '')
```

      Tento příkaz můžete také spustit v jazyce Jacl. Další informace o tom, jak to provést, naleznete v tématu *Zajištění toho, aby servery používaly nejnovější dostupnou úroveň údržby IBM MQ adaptéru prostředků* v dokumentaci k produktu WebSphere Application Server .

   d) Vyhledejte zprávu `WMSG1703I` v zobrazeném výstupu z příkazu a zkontrolujte úroveň adaptéru prostředků.

      Například pro WebSphere Application Server 7.0.1 Fix Pack 5by zpráva měla být:

      ```
      WMSG1703I: Verze implementace RAR 7.0.1.3-k701-103-100812
      ```

      Tato zpráva ukazuje, že verze je 7.0.1.3-k701-103-100812, což je správná úroveň adaptéru prostředků pro tuto opravnou sadu. Pokud se však místo toho zobrazí následující zpráva, znamená

to, že musíte upravit adaptér prostředků na správnou úroveň údržby pro produkt WebSphere Application Server 7.0.1 Fix Pack 5.

```
WMSG1703I: Verze implementace RAR 7.0.0.0-k700-L080820
```

3. Zkopírujte následující skript Jython do souboru s názvem `convertWMQRA.py` a poté jej uložte do kořenového adresáře profilu, například `C:\Program Files\IBM\WebSphere\AppServer1\bin`.

```
ras = AdminUtilities.convertToList(AdminConfig.list('J2CResourceAdapter'))

for ra in ras :
  desc = AdminConfig.showAttribute(ra, "description")
  if (desc == "WAS 7.0 Built In MQ Resource Adapter") or (desc == "WAS 7.0.0.1 Built In MQ Resource
Adapter"):
    print "Updating archivePath and classpath of " + ra
    AdminConfig.modify(ra, [['archivePath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar"]])
    AdminConfig.unsetAttributes(ra, ['classpath'])
    AdminConfig.modify(ra, [['classpath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar"]])
    AdminConfig.save()
  #end if
#end for
```

Tip: Při ukládání souboru se ujistěte, že je uložen jako soubor python, nikoli jako textový soubor.

4. Pomocí nástroje WebSphere Application Server wsadmin spusťte skript Jython, který jste právě vytvořili.

   Otevřete příkazový řádek a přejděte do adresáře `\bin` v domovském adresáři pro adresář WebSphere Application Server, například `C:\Program Files\IBM\WebSphere\AppServer1\bin` , pak zadejte následující příkaz a stiskněte klávesu Return:

   ```
   wsadmin -lang jython -f convertWMQRA.py
   ```

   Pokud k tomu budete vyzváni, zadejte své uživatelské jméno a heslo.

   Poznámka: Spustíte-li skript pro profil, který je součástí konfigurace síťové implementace, skript aktualizuje všechny profily, které je třeba v dané konfiguraci aktualizovat. Úplná resynchronizace může být nezbytná, pokud máte již existující nekonzistence konfiguračního souboru.

5. Pokud pracujete v konfiguraci síťové implementace, ujistěte se, že jsou agenti uzlu plně synchronizováni. Další informace naleznete v tématu Synchronizace uzlů pomocí skriptovacího nástroje wsadmin nebo přidání, správa a odebrání uzlů.
6. Zastavte všechny servery v profilu. Pokud je profil součástí konfigurace síťové implementace, zastavte také všechny členy klastru v konfiguraci, zastavte všechny agenty uzlů v konfiguraci a zastavte správce implementace. Pokud profil obsahuje administrativního agenta, zastavte administrativního agenta.
7. Spusťte příkaz **osgiCfgInit** z adresáře *profile_root*/bin .

   Příkaz `osgiCfgInit` resetuje mezipaměť tříd používanou běhovým prostředím OSGi. Pokud je profil součástí konfigurace síťové implementace, spusťte příkaz **osgiCfgInit** z adresáře `profile_root/bin` každého profilu, který je součástí konfigurace.
8. Restartujte všechny servery v profilu. Pokud je profil součástí konfigurace síťové implementace, restartujte také všechny členy klastru v konfiguraci, restartujte všechny agenty uzlů v konfiguraci a restartujte správce implementace. Pokud profil obsahuje administrativního agenta, restartujte jej.
9. Opakujte krok 2 a zkontrolujte, zda je adaptér prostředků nyní na správné úrovni.

Jak pokračovat dále

Pokud po provedení kroků popsaných v tomto tématu narazíte na problémy a dříve jste použili tlačítko **Aktualizovat adaptér prostředků** na panelu Nastavení poskytovatele JMS v administrativní konzole WebSphere Application Server k aktualizaci adaptéru prostředků IBM MQ na všech uzlech ve vašem prostředí, je možné, že máte problém popsaný v APAR PM10308.

Související pojmy

Použití adaptéru prostředků IBM MQ

Související informace pro WebSphere Application Server 8.5.5

Zajištění, aby servery používaly nejnovější dostupnou úroveň údržby adaptéru prostředků IBM MQ
Synchronizace uzlů pomocí skriptovacího nástroje wsadmin
Přidání, správa a odebrání uzlů
Nastavení poskytovatele JMS

Konfigurace vlastnosti JMS PROVIDERVERSION

Poskytovatel systému zpráv IBM MQ má tři provozní režimy: normální režim, normální režim s omezeními a režim migrace. Můžete nastavit vlastnost JMS **PROVIDERVERSION** a vybrat, který z těchto režimů aplikace JMS používá k publikování a odběru.

Informace o této úloze

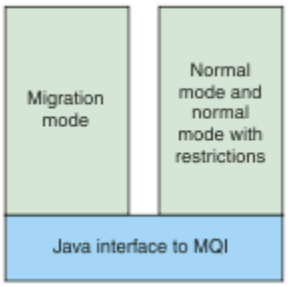
Výběr režimu operace poskytovatele systému zpráv IBM MQ lze primárně řídit nastavením vlastnosti PROVIDERVERSION továrny připojení. Režim operace lze také vybrat automaticky, pokud nebyl zadán režim.

Vlastnost **PROVIDERVERSION** rozlišuje mezi třemi režimy operací poskytovatele systému zpráv IBM MQ :

Normální režim poskytovatele systému zpráv IBM MQ
Normální režim používá všechny funkce správce front IBM MQ k implementaci služby JMS. Tento režim je optimalizovaný pro použití rozhraní API a funkčnosti JMS 2.0.

IBM MQ s omezeními
Normální režim s omezeními používá rozhraní API JMS 2.0 , nikoli však nové funkce, tj. sdílené odběry, zpožděné doručení a asynchronní odesílání.

Režim migrace poskytovatele systému zpráv IBM MQ
V režimu migrace se můžete připojit ke správci front IBM MQ 8.0 nebo novějšímu, ale nepoužívají se žádné funkce správce front produktu IBM WebSphere MQ 7.0 nebo novějšího, například dopředné čtení a proudové zpracování.



Obrázek 89. Režimy poskytovatele systému zpráv

Procedura

Chcete-li konfigurovat vlastnost **PROVIDERVERSION** pro specifickou továrnu připojení, postupujte takto:

- Chcete-li konfigurovat vlastnost **PROVIDERVERSION** pomocí produktu IBM MQ Explorer, postupujte podle části Konfigurace správců front a objektů.
- Chcete-li konfigurovat vlastnost **PROVIDERVERSION** pomocí nástroje pro administraci JMS , postupujte podle části Konfigurace správců front a objektů.
- Chcete-li nakonfigurovat vlastnost **PROVIDERVERSION** v aplikaci JMS pomocí rozšíření IBM JMS nebo rozšíření IBM MQ JMS , prohlédněte si témaVytvoření a konfigurace továren připojení a míst určení v IBM MQ classes for JMS aplikaci.

Chcete-li přepsat nastavení režimu poskytovatele továrny připojení pro všechny továrny připojení v prostředí JVM, postupujte takto:

- Chcete-li přepsat nastavení režimu poskytovatele továrny připojení, použijte vlastnost `com.ibm.msg.client.wmq.overrideProviderVersion`

  Pokud nemůžete změnit továrnu připojení, kterou používáte, můžete použít vlastnost `com.ibm.msg.client.wmq.overrideProviderVersion` k potlačení jakéhokoli nastavení v továrně připojení. Tento přepis platí pro všechny továrny připojení v prostředí JVM, ale skutečné objekty továrny připojení se nezmění.

Související pojmy

Odstraňování problémů s verzí poskytovatele JMS

Související odkazy

PROVIDERVERSION

Vlastnosti továrny připojení

Závislosti mezi vlastnostmi objektů IBM MQ classes for JMS

Provozní režimy poskytovatele systému zpráv IBM MQ

Nastavením vlastnosti PROVIDERVERSION pro továrnu připojení na odpovídající hodnotu můžete vybrat, který provozní režim poskytovatele systému zpráv IBM MQ aplikace JMS používá k publikování a odběru. V některých případech je vlastnost PROVIDERVERSION nastavena jako nespecifikovaná, v takovém případě klient JMS používá algoritmus k určení, který režim operace má použít.

PROVIDERVERSION Hodnoty vlastností

Vlastnost **PROVIDERVERSION** továrny připojení můžete nastavit na libovolnou z následujících hodnot:

8 - Normální režim
Aplikace JMS používá normální režim. Tento režim používá všechny funkce IBM MQ správce front k implementaci JMS.

7 - Normální režim s omezeními
Aplikace JMS používá normální režim s omezeními. Tento režim používá rozhraní JMS 2.0 API, ale ne nové funkce, jako sdílení odběrů, odložené doručení nebo asynchronní odeslání.

6 - Režim migrace
Aplikace JMS používá režim migrace. V režimu migrace produkt IBM MQ classes for JMS používá funkce a algoritmy podobné těm, které jsou dodávány s produktem IBM WebSphere MQ 6.0.

unurčený (výchozí hodnota)
Klient JMS používá algoritmus k určení, který režim operace se používá.

Vámi zadaná hodnota ve vlastnosti **PROVIDERVERSION** musí být řetězec. Pokud zadáte volbu 8, 7 nebo 6, můžete to provést v některém z následujících formátů:

- V.R.M.F
- V.R.M
- V.R
- V

kde V, R, M a F jsou celá čísla větší nebo rovná nule. Hodnoty R, M a F jsou nepovinné a můžete je použít k upřesnění v případě potřeby řízení s vysokou úrovní granularity. Chcete-li například použít úroveň **PROVIDERVERSION** 7, můžete nastavit **PROVIDERVERSION** = 7, `7.0`, `7.0.0` nebo `7.0.0.0`.

Typy objektů továrny připojení

Vlastnost **PROVIDERVERSION** můžete nastavit pro následující typy objektů továrny připojení:

- MQConnectionFactory
- Továrna MQQueueConnection
- Továrna MQTopicConnection
- MQXAConnectionFactory

- Továrna MQXAQueueConnection
- Továrna MQXAQueueConnection
- Továrna MQXAQueueConnection
- Továrna MQXATopicConnection

Další informace o těchto různých typech továrny připojení viz “Konfigurace objektů JMS a Jakarta Messaging pomocí nástrojů pro administraci” na stránce 664.

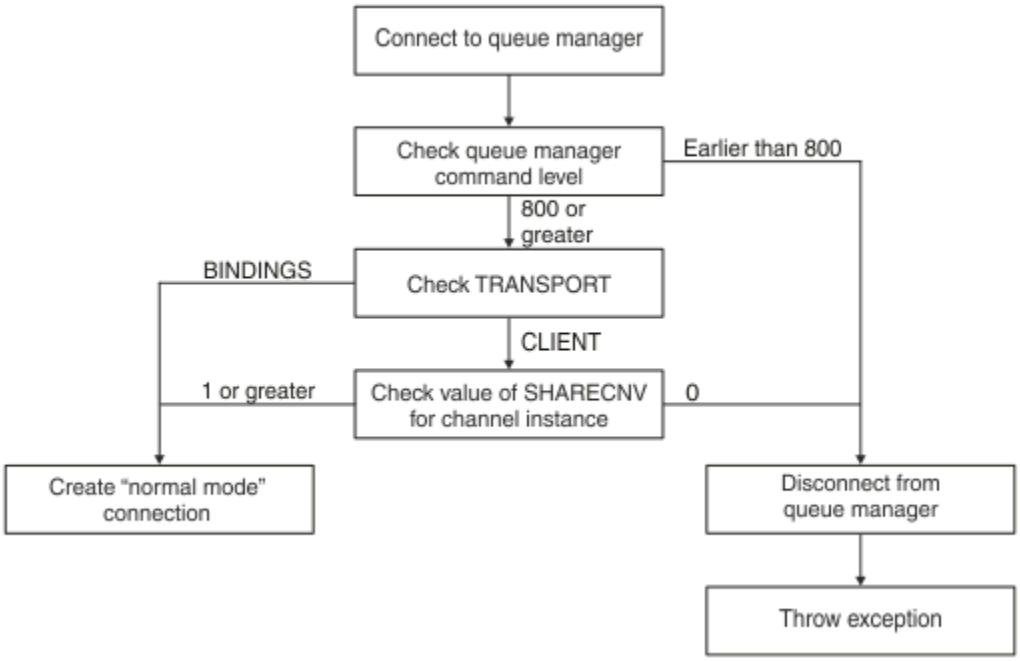
Související pojmy

IBM MQ poskytovatel systému zpráv

PROVIDERVERSION Normální režim

Normální režim používá všechny funkce správce front IBM MQ k implementaci služby JMS. Tento režim je optimalizovaný pro použití rozhraní API a funkčnosti JMS 2.0.

Následující graf toku zobrazuje kontroly, které klient JMS provádí, aby určil, zda lze vytvořit připojení v normálním režimu.



Obrázek 90. Normální režim PROVIDERVERSION

Pokud má správce front určený v nastavení továrny připojení úroveň příkazu 800 nebo vyšší a vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS, vytvoří se připojení v normálním režimu bez kontroly dalších vlastností.

Pokud má správce front určený v nastavení továrny připojení úroveň příkazu 800 nebo vyšší a vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, bude také zaškrtnuta vlastnost **SHARECNV** v kanálu připojení serveru. Tato kontrola je vyžadována, protože normální režim poskytovatele systému zpráv IBM MQ používá funkci sdílení konverzací. Proto, aby byl pokus o připojení v normálním režimu úspěšný, musí mít vlastnost **SHARECNV** , která řídí počet konverzací, které lze sdílet, hodnotu 1 nebo vyšší.

Pokud jsou všechny kontroly zobrazené v grafu toku úspěšné, je vytvořeno připojení v normálním režimu ke správci front a lze použít všechna rozhraní API a funkce produktu JMS 2.0 , tj. asynchronní odeslání, zpožděné doručení a sdílený odběr.

Pokus o vytvoření připojení v normálním režimu se nezdaří z jedné z následujících příčin:

- Správce front určený v nastavení továrny připojení má úroveň příkazu starší než 800. V tomto případě metoda `createConnection` selže s výjimkou `JMSFMQ0003`.

- Vlastnost **SHARECNV** kanálu připojení serveru je nastavena na hodnotu 0. Pokud tato vlastnost nemá hodnotu 1 nebo vyšší, metoda `createConnection` selže s výjimkou `JMSCC5007`.

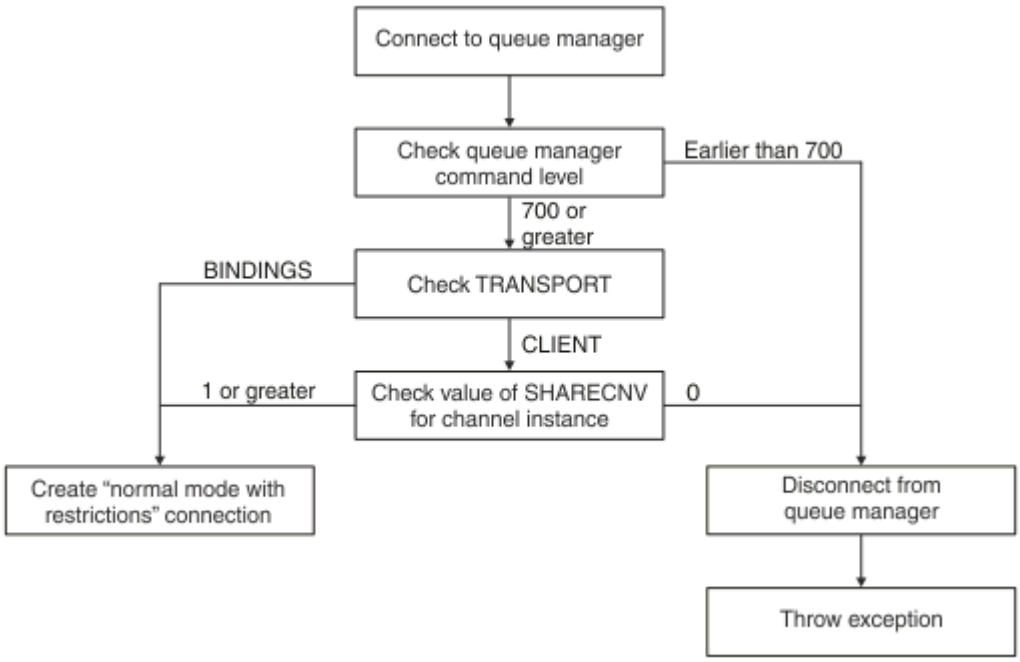
Související odkazy

Závislosti mezi vlastnostmi objektů IBM MQ classes for JMS
DEFINE CHANNEL (vlastnost SHARECNV)
TRANSPORT

PROVIDERVERSION normální režim s omezeními

Normální režim s omezeními používá rozhraní API JMS 2.0 , ale ne nové funkce IBM MQ 8.0 nebo novější, jako jsou sdílené odběry, zpožděné doručení nebo asynchronní odeslání.

Následující graf toku zobrazuje kontroly, které klient JMS provádí, aby určil, zda lze vytvořit normální režim s omezením připojení.



Obrázek 91. PROVIDERVERSION normální režim s omezeními

Pokud má správce front určený v nastavení továrny připojení úroveň příkazu 700 nebo vyšší a vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS, vytvoří se připojení v normálním režimu bez zaškrtnutí dalších vlastností.

Pokud má správce front určený v nastavení továrny připojení úroveň příkazu 700 nebo vyšší a vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, bude také zaškrtnuta vlastnost **SHARECNV** v kanálu připojení serveru. Tato kontrola je potřebná, protože normální režim poskytovatele systému zpráv IBM MQ s omezeními používá funkci sdílení konverzací. Proto, aby byl pokus o připojení v normálním režimu s omezeními úspěšný, musí mít vlastnost **SHARECNV** , která řídí počet konverzací, které lze sdílet, hodnotu 1 nebo vyšší.

Pokud jsou všechny kontroly zobrazené v grafu toku úspěšné, vytvoří se normální režim s omezením připojení ke správci front a poté můžete použít rozhraní API JMS 2.0 , ale ne funkce asynchronního odeslání, zpožděného doručení nebo sdíleného odběru.

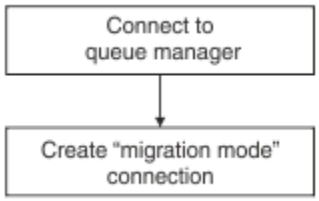
Pokus o vytvoření normálního režimu s omezením připojení selže z jedné z následujících příčin:

- Správce front určený v nastavení továrny připojení má úroveň příkazu dřívější než 700. V tomto případě metoda `createConnection` selže s výjimkou `JMSFCC5008`.
- Vlastnost **SHARECNV** kanálu připojení serveru je nastavena na hodnotu 0. Pokud tato vlastnost nemá hodnotu 1 nebo vyšší, metoda `createConnection` selže s výjimkou `JMSCC5007`.

Související odkazy
Závislosti mezi vlastnostmi objektů IBM MQ classes for JMS
DEFINE CHANNEL (vlastnost SHARECNV)
TRANSPORT

PROVIDERVERSION režim migrace

Pro režim migrace produkt IBM MQ classes for JMS používá funkce a algoritmy podobné těm, které jsou dodávány s produktem IBM WebSphere MQ 6.0, jako např. publikování/odběr ve frontě, výběr implementovaný na straně klienta, nemultiplexní kanály a systém výzev použitý k implementaci listenerů.



Obrázek 92. Režim migrace PROVIDERVERSION

Chcete-li se připojit k produktu WebSphere Message Broker 6.0 nebo WebSphere Message Broker 6.1 pomocí produktu IBM MQ Enterprise Transport verze 6.0, musíte použít režim migrace.

Ke správci front IBM MQ 8.0 se můžete připojit pomocí režimu migrace, ale nejsou použity žádné nové funkce správce front IBM MQ classes for JMS , například dopředné čtení nebo kontinuální zpracování. Máte-li klienta IBM MQ 8.0 nebo novějšího, který se připojuje ke správci front systému IBM MQ 8.0 nebo novějšímu na distribuované platformě z/OS nebo IBM MQ for z/OS 8.0 či novějšímu správci front, pak výběr zpráv provádí správce front a nikoli klientský systém.

Je-li zadán režim migrace poskytovatele systému zpráv IBM MQ a produkt IBM MQ classes for JMS se pokusí použít libovolné rozhraní API JMS 2.0 , volání metody rozhraní API se nezdaří s výjimkou `JMSCC5007`.

Související odkazy
Závislosti mezi vlastnostmi objektů IBM MQ classes for JMS
TRANSPORT

PROVIDERVERSION nespecifikováno

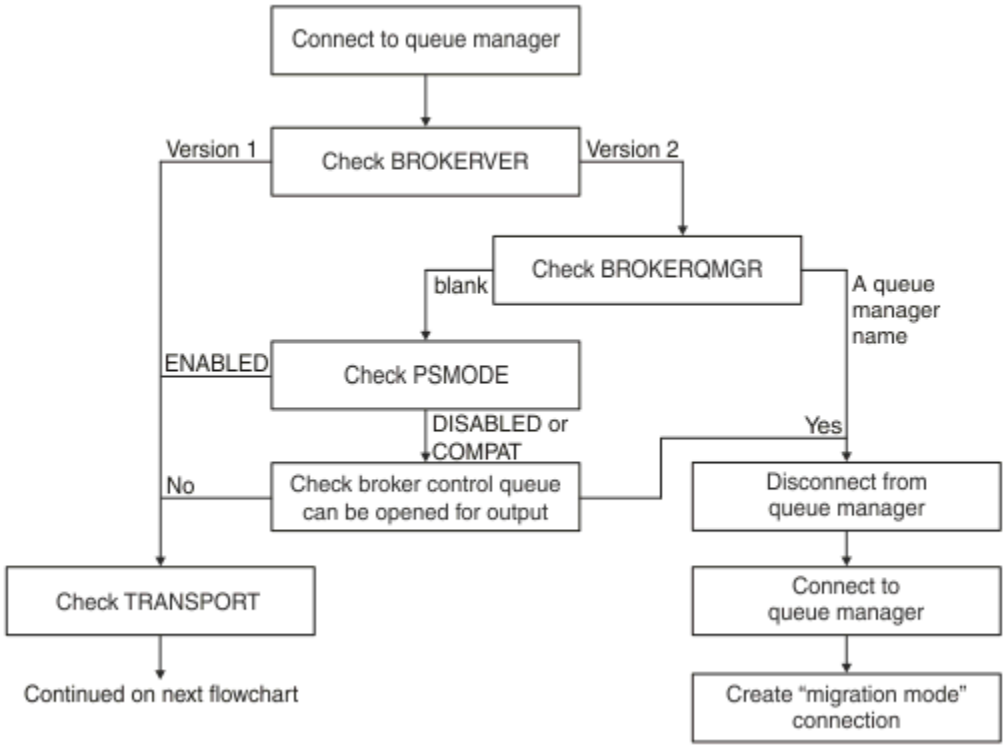
Není-li vlastnost **PROVIDERVERSION** továrny připojení určena, klient produktu JMS použije algoritmus k určení, který režim operace se používá pro připojení ke správci front. Továrna připojení, která byla vytvořena v oboru názvů JNDI s předchozí verzí produktu IBM MQ classes for JMS , vezme neurčenou hodnotu při použití továrny připojení s novou verzí produktu IBM MQ classes for JMS.

Není-li vlastnost **PROVIDERVERSION** určena, použije se algoritmus při volání metody `createConnection` . Algoritmus kontroluje řadu vlastností továrny připojení a zjišťuje, zda je vyžadován normální režim poskytovatele systému zpráv IBM MQ , normální režim s omezeními nebo režim migrace poskytovatele systému zpráv IBM MQ . Nejprve je vždy proveden pokus o normální režim a poté o normální režim s omezeními. Pokud nelze vytvořit žádný z těchto typů připojení, klient JMS se odpojí od správce front a poté se znovu připojí ke správci front a pokusí se o připojení v režimu migrace.

Kontrola vlastností BROKERVER, BROKERQMGR, PSMODEa BROKERCONQ

Kontrola hodnot vlastností začíná vlastností **BROKERVER** , jak ukazuje Obrázek 1.

Je-li vlastnost **BROKERVER** nastavena na hodnotu V1, bude vlastnost **TRANSPORT** zaškrtnuta jako další, jak ukazuje Obrázek 2. Je-li však vlastnost **BROKERVER** nastavena na hodnotu V2, provede se před kontrolou vlastnosti **TRANSPORT** další kontrola uvedená na obrázku Obrázek 1 .



Obrázek 93. PROVIDERVERSION nespecifikováno

Je-li vlastnost **BROKERVER** nastavena na hodnotu V2, musí být vlastnost **BROKERQMGR** `prázdná`, aby bylo možné připojení v normálním režimu. Dále musí být atribut **PSMODE** ve správci front nastaven na hodnotu ENABLED nebo nesmí být možné otevřít frontu řízení zprostředkovatele určenou vlastností **BROKERCONQ** pro výstup.

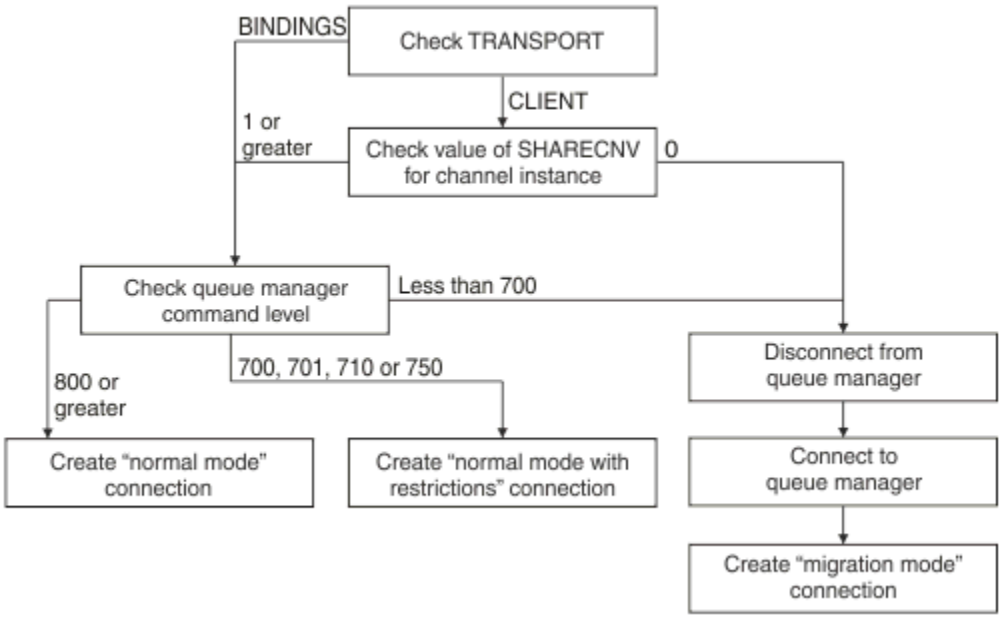
Pokud jsou hodnoty vlastností nastaveny podle potřeby pro připojení v normálním režimu, kontrola dalších přesunů k vlastnosti **TRANSPORT** , jak ukazuje Obrázek 2.

Nejsou-li hodnoty vlastností nastaveny podle potřeby pro připojení v normálním režimu, klient JMS se odpojí od správce front a poté se znovu připojí a vytvoří připojení v režimu migrace. K tomu dochází v následujících případech:

- Je-li vlastnost **BROKERQMGR** `prázdná` a atribut **PSMODE** ve správci front je nastaven na hodnotu COMPAT nebo DISABLED a řídicí frontu zprostředkovatele určenou vlastností **BROKERCONQ** lze otevřít pro výstup (tj. MQOPEN pro úspěšné výstupy).
- Pokud vlastnost **BROKERQMGR** uvádí název fronty.

Kontrola vlastnosti TRANSPORT a úrovně příkazu

Obrázek 2 ukazuje kontroly provedené pro vlastnost **TRANSPORT** a úroveň příkazu správce front.



Obrázek 94. PROVIDERVERSION nespecifikováno (pokračování)

Připojení v normálním režimu se vytvoří v jednom z následujících případů:

- Vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS a správce front má úroveň příkazu 800 nebo vyšší.
- Vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, vlastnost **SHARECNV** v kanálu připojení serveru má hodnotu 1 nebo vyšší a správce front má úroveň příkazu 800 nebo vyšší.

Pokud má správce front úroveň příkazu 750, vytvoří se normální režim s omezením připojení ke správci front.

Připojení v režimu migrace se také vytvoří, pokud je vlastnost **TRANSPORT** nastavena na hodnotu CLIENT a vlastnost **SHARECNV** v kanálu připojení serveru má hodnotu 0.

Související odkazy

Závislosti mezi vlastnostmi objektů IBM MQ classes for JMS
ALTER QMGR (atribut PSMODE)
BROKERCONQ
BROKERQMGR
BROKERVER
DEFINE CHANNEL (vlastnost SHARECNV)
TRANSPORT

Konfigurace informací o verzi poskytovatele v adresáři WebSphere Application Server

Chcete-li konfigurovat informace o verzi poskytovatele v produktu WebSphere Application Server, můžete použít buď administrativní konzolu, nebo příkazy wsadmin.

Postup

Chcete-li konfigurovat informace o verzi poskytovatele pro továrnu připojení IBM MQ nebo objekt specifikace aktivace v produktu WebSphere Application Server, prohlédněte si *Související informace* , kde naleznete odkazy na další informace v dokumentaci k produktu WebSphere Application Server .

Související informace pro WebSphere Application Server 8.5.5
Nastavení továrny připojení poskytovatele systému zpráv IBM MQ
createWMQConnectionFactory příkaz
Nastavení specifikace aktivace poskytovatele systému zpráv IBM MQ
createWMQActivationSpec příkaz
Související informace pro WebSphere Application Server 8.0.0
Nastavení továrny připojení poskytovatele systému zpráv IBM MQ
createWMQConnectionFactory příkaz
Nastavení specifikace aktivace IBM MQ
createWMQActivationSpec příkaz
Související informace pro WebSphere Application Server 7.0.0
Nastavení továrny připojení poskytovatele systému zpráv IBM MQ
createWMQConnectionFactory příkaz
Nastavení specifikace aktivace IBM MQ
createWMQActivationSpec příkaz

Odebrání WebSphere Application Server trvalých odběrů

Při použití poskytovatele systému zpráv IBM MQ s aplikacemi WebSphere Application Server 7.0 a WebSphere Application Server 8.0nejsou odebrány trvalé odběry vytvořené aplikacemi objektů typu message-driven bean svázanými se specifikacemi aktivace. Trvalé odběry lze odebrat buď pomocí obslužného programu příkazového řádku IBM MQ Explorer , nebo pomocí obslužného programu IBM MQ .

Informace o této úloze

Aplikaci objektu typu message-driven bean, která odebírá trvalý odběr, lze konfigurovat tak, aby používala buď port modulu listener, nebo specifikaci aktivace, za předpokladu, že je aplikace spuštěna v rámci instance WebSphere Application Server 7.0 nebo WebSphere Application Server 8.0 , která používá pro připojení k produktu IBM MQhodnotu Normální režim poskytovatele systému zpráv IBM MQ .

Pokud je aplikace objektu typu message-driven bean svázána s portem modulu listener, poskytovatel systému zpráv IBM MQ vytvoří trvalý odběr pro aplikaci při prvním spuštění aplikace. Trvalý odběr je odebrán při odinstalaci aplikace objektu typu message-driven bean z aplikačního serveru a restartování aplikačního serveru.

Aplikace objektu typu message-driven bean, která je svázána se specifikací aktivace, pracuje poněkud odlišným způsobem. Trvalý odběr je pro aplikaci vytvořen při prvním spuštění aplikace. Trvalý odběr však není při odinstalaci aplikace a restartování aplikačního serveru odebrán.

To může vést k počtu trvalých odběrů, které zbývají na stroji IBM MQ Publikovat/Odebírat pro aplikace, které již nejsou nainstalovány v systému WebSphere Application Server . Tyto odběry jsou označovány jako "osiřelé odběry" a mohou vést k problémům se správcem front při spuštění stroje publikování/odběru.

Je-li zpráva publikována v tématu, stroj publikování/odběru produktu IBM MQ vytvoří kopii této zprávy pro každý trvalý odběr, který je v daném tématu registrován, a vloží ji do interní fronty. Aplikace používající tento trvalý odběr pak vyzvednou a spotřebují zprávu z této interní fronty.

Pokud již není nainstalována aplikace objektu typu message-driven bean, která tento trvalý odběr používala, budou i nadále prováděny kopie publikovaných zpráv pro aplikaci. Tyto zprávy však nebudou nikdy zpracovány, což znamená, že v interní frontě může zůstat velký počet zpráv, které nebudou nikdy odebrány.

Než začnete

Odběry, které jsou registrovány ve stroji publikování/odběru produktu IBM MQ , budou mít k sobě přidružen název odběru.

Trvalé odběry vytvořené poskytovatelem systému zpráv WebSphere Application Server IBM MQ pro objekty typu message-driven bean, které jsou vázány na specifikace aktivace, budou mít název odběru v následujícím formátu:

```
JMS:queue manager name:client identifier:subscription name
```

Kde:

Název správce front
Jedná se o název správce front IBM MQ , kde je spuštěn stroj publikování/odběru.

Identifikátor klienta
Jedná se o hodnotu vlastnosti ID klienta specifikace aktivace, se kterou je objekt typu message-driven bean svázán.

Název odběru
Jedná se o hodnotu vlastnosti odběru specifikace aktivace pro specifikaci aktivace, pro kterou byla aplikace objektu typu message-driven bean konfigurována pro použití.

Předpokládejme například, že máme specifikaci aktivace, která byla nastavena pro připojení ke správci front testQM. Specifikace aktivace má nastaveny následující vlastnosti:

- ID klienta = testClientID
- Název odběru = durableSubscription1

Pokud je objekt typu message-driven bean, který odebírá trvalý odběr, svázán s touto specifikací aktivace, vytvoří se odběr ve stroji IBM MQ publish/subscribe ve správci front testQM , který má následující název odběru:

- JMS:testQM:testClientID:durableSubscription1

Odběry, které byly registrovány ve stroji publikování/odběru produktu IBM MQ pro daného správce front, lze zobrazit jedním z následujících způsobů:

- První volbou je použití Průzkumníka produktu MQ . Pokud byl produkt MQ Explorer připojen ke správci front, který se používá pro práci publikování/odběru, lze seznam odběratelů, kteří jsou aktuálně registrováni ve stroji publikování/odběru, zobrazit klepnutím na položku `IBM WebSphere MQ ->queue manager name-> Subscriptions` v navigačním podokně.
- Druhým způsobem zobrazení odběrů, které byly registrovány pomocí stroje publikování/odběru, je použití IBM MQ obslužného programu příkazového řádku **runmqsc** a spuštění příkazu **display sub**. Chcete-li to provést, spusťte příkazový řádek, přejděte do adresáře *WebSphere MQ*\bin a zadejte následující příkaz pro spuštění **runmqsc**:

  – `runmqsc queue manager name`

  Po spuštění obslužného programu **runmqsc** zadáním následujícího příkazu vypište všechny trvalé odběry, které jsou aktuálně registrovány ve stroji publikování/odběru spuštěném ve správci front, k němuž se produkt **runmqsc** připojil:

  – `display sub(*) durable`

Chcete-li zkontrolovat, zda jsou trvalé odběry registrované u strojů publikování/odběru stále aktivní, postupujte takto:

1. Vygenerujte seznam trvalých odběrů, které byly registrovány ve stroji publikování/odběru.
2. Pro každý trvalý odběr:
   - Podívejte se na název trvalého odběratele a poznamenejte si hodnotu *identifikátor klienta* a *název odběru* .
   - Podívejte se na systémy WebSphere Application Server , které se připojují k tomuto stroji publikování/odběru. Zjistěte, zda jsou definovány nějaké specifikace aktivace, které mají vlastnost ID klienta odpovídající hodnotě *identifikátor klienta* a vlastnosti názvu odběru odpovídající *názvu odběru*.

- Nejsou-li nalezeny žádné specifikace aktivace, které mají vlastnosti ID klienta a název odběru odpovídající polím *identifikátor klienta* a *název odběru* v názvu odběru IBM MQ , nejsou k dispozici žádné specifikace aktivace používající tento trvalý odběr. Trvalý odběr lze odstranit.
- Je-li definována specifikace aktivace, která odpovídá názvu trvalého odběru, je třeba provést závěrečnou kontrolu, zda existuje aplikace objektu typu message-driven bean používající tuto specifikaci aktivace. Postupujte takto:
  - Poznamenejte si název JNDI pro specifikaci aktivace, která získala trvalý odběr, který právě hledáte.
  - Zobrazte podokno Konfigurace v administrativní konzole produktu WebSphere Application Server pro každou nainstalovanou aplikaci objektu typu message-driven bean.
  - V podokně Konfigurace klepněte na odkaz na vazby modulu listener objektu typu message-driven bean.
  - Zobrazí se tabulka s informacemi o aplikaci objektu typu message-driven bean. Je-li ve sloupci Vazby vybrán přepínač specifikace aktivace a pole Název cílového prostředku JNDI obsahuje název JNDI pro specifikaci aktivace, která převzala trvalý odběr, je odběr stále používán a nelze jej odstranit.
  - Pokud nelze nalézt žádné aplikace objektů typu message-driven bean, které používají specifikaci aktivace, lze trvalý odběr odstranit.

Postup

Po identifikaci "osiřelého" trvalého odběru jej lze odstranit pomocí obslužného programu IBM MQ Explorer nebo IBM MQ obslužného programu příkazového řádku **runmqsc**.

Chcete-li odstranit "osiřelý" trvalý odběr pomocí konzoly IBM MQ Explorer, postupujte takto:

1. Zvýraznit položku pro odběr
2. Klepněte pravým tlačítkem myši na položku a vyberte volbu **Odstranit ...** z nabídky. Zobrazí se okno s potvrzením.
3. Zkontrolujte, zda je název odběru zobrazený v potvrzovacím okně správný, a klepněte na tlačítko **Ano**.

Produkt IBM MQ Explorer nyní odstraní odběr ze stroje publikování/odběru a vyčistí všechny interní prostředky, které jsou k němu přidruženy (například nezpracované zprávy, které byly publikovány pro téma, pro které byl trvalý odběr registrován).

Chcete-li odstranit "osiřelý" trvalý odběr pomocí IBM MQ obslužného programu příkazového řádku **runmqsc**, musíte spustit příkaz **delete sub** :

1. Otevřít relaci příkazového řádku
2. Přejděte do adresáře *IBM MQ*\bin .
3. Spusťte příkaz **runmqsc**zadáním následujícího příkazu:

```
runmqsc queue manager name
```

4. Po spuštění obslužného programu **runmqsc** zadejte:

```
delete sub(Subscription name)
```

kde *Název odběru* je název trvalého odběru ve tvaru:

- JMS:*queue manager name*:*client identifier*:*subscription name*

Konfigurace produktu Managed File Transfer

Po instalaci můžete nakonfigurovat funkce produktu Managed File Transfer .

Můžete využít výhod řešení vysoké dostupnosti IBM MQ ke zlepšení odolnosti konfigurace produktu Managed File Transfer . Pokud vaši agenti používají správce front replikovaných dat (RDQM), musíte je nakonfigurovat tak, aby používaly funkci plovoucí adresy IP. To znamená, že agenti používají stejnou adresu IP ke komunikaci s jakoukoli ze tří instancí RDQM, která je momentálně spuštěna, a automaticky se znovu připojí při překonání selhání (viz Vysoká dostupnost RDQM a Vytvoření a odstranění plovoucí adresy IP). Používáte-li řešení správce front s více instancemi, budou aplikace při komunikaci s každou instancí používat jinou adresu IP, která je obsluhována opětným připojením klienta při překonání selhání (viz Správci front s více instancemi a Opětovné připojení kanálu a klienta).

Související pojmy

Rady a tipy pro použití Managed File Transfer

Související úlohy

Monitorování prostředků MFT

Přizpůsobení produktu MFT pomocí uživatelských procedur

Konfigurace souboru MQMFTCredentials.xml

zabezpečeníManaged File Transfer

Určení programů, které se mají spustit s MFT

odstraňování problémůManaged File Transfer

Správa serveruManaged File Transfer

Související odkazy

MFT příkazy

Soubor MFT`agent.properties`

Obnova a restart MFT

Volby konfigurace MFT na platformě Multiplatforms

Produkt Managed File Transfer poskytuje sadu souborů vlastností, které obsahují klíčové informace o vašem nastavení a jsou nezbytné pro operaci. Tyto soubory vlastností se nacházejí v konfiguračním adresáři, který jste definovali při instalaci produktu.

Můžete mít více sad voleb konfigurace, každá sada voleb konfigurace obsahuje sadu adresářů a souborů vlastností. Hodnoty definované v těchto souborech vlastností jsou použity jako výchozí parametry pro všechny příkazy Managed File Transfer , pokud explicitně nezadáte jinou hodnotu na příkazovém řádku.

Chcete-li změnit výchozí sadu voleb konfigurace, kterou používáte, můžete použít příkaz **fteChangeDefaultConfigurationOptions** . Chcete-li změnit sadu voleb konfigurace, kterou používáte pro jednotlivý příkaz, můžete použít parametr **-p** s libovolným příkazem Managed File Transfer .

Název sady voleb konfigurace je název koordinačního správce front a doporučuje se, aby se tento název nezměnil. Je však možné změnit název sady voleb konfigurace, ale musíte změnit název adresářů `config` a `logs` . V následujících příkladech je název sady voleb konfigurace reprezentován jako *coordination_qmgr_name*.

Adresářová struktura voleb konfigurace

Když konfigurujete produkt, adresáře a soubory vlastností se vytvoří v následující struktuře v konfiguračním adresáři. Tyto adresáře a soubory vlastností můžete také změnit pomocí následujících příkazů: **fteSetupCoordination**, **fteSetupCommands**, **fteChangeDefaultConfiguration**a **fteCreateAgent**.

```
MQ_DATA_PATH/mqft/
    config/
       coordination_qmgr_name/
            coordination.properties
            command.properties
            agents/
               agent_name/
                    agent.properties
                    exits
            loggers/
```

```
                logger_name
                     logger.properties
    installations/
       installation_name/
            installation.properties
```

Adresář *coordination_qmgr_name* je adresář voleb konfigurace. V konfiguračním adresáři může být více než jeden adresář voleb konfigurace. Adresář *agent_name* je adresář agenta. Kromě toho, že obsahuje soubor `agent.properties` , obsahuje tento adresář adresář `exits` , což je výchozí umístění pro uživatelské procedury a různé soubory XML generované příkazy **`fteCreateBridgeAgent`** a **`fteCreateCDAgent`** . V adresáři `agents` sady voleb konfigurace může být více než jeden adresář agenta.

soubory vlastností

installation.properties
Soubor `installation.properties` uvádí název výchozí sady voleb konfigurace. Tato položka ukazuje Managed File Transfer na strukturovanou sadu adresářů a souborů vlastností, které obsahují konfiguraci, která se má použít. Obvykle je název sady voleb konfigurace názvem přidruženého koordinačního správce front. Další informace o souboru `installation.properties` viz Soubor MFT installation.properties.

coordination.properties
Soubor `coordination.properties` uvádí podrobnosti připojení ke koordinačnímu správci front. Vzhledem k tomu, že několik instalací produktu Managed File Transfer může sdílet stejného koordinačního správce front, můžete použít symbolický odkaz na společný soubor `coordination.properties` na sdílené jednotce. Další informace o souboru `coordination.properties` viz Soubor MFT coordination.properties.

command.properties
Soubor MFT command.properties určuje správce front příkazů, ke kterému se má připojit při zadávání příkazů, a informace, které produkt Managed File Transfer vyžaduje pro kontaktování tohoto správce front. Další informace o souboru `command.properties` viz Soubor MFT command.properties.

agent.properties
Každý Managed File Transfer Agent má svůj vlastní soubor vlastností `agent.properties`, který musí obsahovat informace, které agent používá pro připojení ke svému správci front. Soubor `agent.properties` může také obsahovat vlastnosti, které mění chování agenta. Další informace o souboru `agent.properties` viz Soubor MFT `agent.properties`.

logger.properties
Soubor `logger.properties` uvádí vlastnosti konfigurace pro moduly protokolování. Další informace o souboru `logger.properties` viz MFT vlastnosti konfigurace modulu protokolování.

Soubory vlastností a kódové stránky

Obsah všech souborů vlastností Managed File Transfer musí zůstat v americké angličtině kvůli omezení na Java. Pokud upravujete soubory vlastností v systému s jinou než americkou angličtinou, musíte použít řídicí posloupnosti Unicode.

Související odkazy
Vlastnosti SSL/TLS pro MFT
Java systémové vlastnosti pro MFT
fteChangeDefaultConfiguration
Příkazy fteSetup: Vytvořte soubor MFT command.properties .
fteSetupKoordinace
fteCreateAgent

z/OS MFT volby konfigurace na z/OS

Volby konfigurace Managed File Transfer v systému z/OS jsou stejné jako volby pro distribuované platformy.

Další informace o volbách konfigurace v systému Multiplatformsviz “Volby konfigurace MFT na platformě Multiplatforms” na stránce 696.

V systému z/OSje umístění konfigurace definováno proměnnou prostředí BFG_DATA. Pokud konfigurace dosud neexistuje v adresáři z/OS UNIX System Services , na který odkazuje BFG_DATA, skript BFGCUSTM JCL datové sady knihovny PDSE příkazu MFT vygeneruje úlohy nezbytné pro vytvoření konfigurace. Konfigurace se pak vytvoří při spuštění těchto generovaných úloh. Vytvoření konfigurace spoléhá na BFG_DATA odkazující na existující adresář, který je přístupný.

Konfiguraci můžete také vytvořit a udržovat pomocí stejných příkazů **fte** , které jsou k dispozici na platformách Multiplatforms i z/OS. Seznam příkazů **fte** viz MFT příkazy .

Související pojmy

“Volby konfigurace MFT na platformě Multiplatforms” na stránce 696
Produkt Managed File Transfer poskytuje sadu souborů vlastností, které obsahují klíčové informace o vašem nastavení a jsou nezbytné pro operaci. Tyto soubory vlastností se nacházejí v konfiguračním adresáři, který jste definovali při instalaci produktu.

“Vytvoření agenta” na stránce 714
Musíte zkopírovat PDSE, abyste učinili PDSE specifickou pro agenta, například *user.MFT.AGENT1*. Zkopírujte PDSE z předchozího agenta nebo konfigurace modulu protokolování, pokud existují. Pokud se jedná o první konfiguraci, zkopírujte PDSE dodávanou s MFT.

“Definování koordinačního správce front” na stránce 712
Produkt Managed File Transfer vyžaduje vytvoření správce front, který bude fungovat jako koordinační správce front.

Související úlohy

z/OS Konfigurace `MQMFTCredentials.xml` na systému z/OS

“Aktualizace existující datové sady příkazu MFT Agent nebo Logger na systému z/OS” na stránce 715
Můžete aktualizovat datovou sadu knihovny PDSE příkazu Managed File Transfer , která je vytvořena z datové sady šablony příkazu Managed File Transfer .

Windows Linux Stažení a konfigurace produktu Redistributable Managed File Transfer components

Produkt Redistributable Managed File Transfer package poskytuje produkt Redistributable Managed File Transfer Agent, který můžete nakonfigurovat pro připojení k existující infrastruktuře IBM MQ a umožnit uživatelům přenos souborů bez nutnosti instalace produktu IBM MQ. Od IBM MQ 9.3.0redistribuovatelný balík také zahrnuje Redistributable Managed File Transfer Logger.

Než začnete

Informace o redistribuovatelných licenčních podmínkách pro Redistributable Managed File Transfer Agent a Redistributable Managed File Transfer Loggernaleznete v tématu IBM MQ Redistribuovatelné komponenty.

Komponenty Redistributable Managed File Transfer package poskytují funkčnost produktu Managed File Transfer s těmito výjimkami:

- V případě agenta Redistributable Managed File Transfer Agentnení připojení v režimu vazeb ke správcům front koordinace, příkazů a agentů podporováno, je třeba použít připojení v režimu klienta. Při zadávání příkazů musíte zadat parametry, které jsou volitelné, používáte-li produkt Managed File Transfer instalovaný jako součást produktu IBM MQ: hostitel správce front, port, název a název kanálu.
- V 9.3.0 Produkt Redistributable Managed File Transfer Logger podporuje pouze moduly protokolování typu FILE, které se připojují pouze v režimu klienta ke koordinačnímu správci front. Připojení v režimu klienta ke koordinačnímu správci front pro modul pro protokolování databáze není podporováno. Pokud požadujete připojení v režimu vazeb, musíte použít standardní instalaci produktu IBM MQ.

- V 9.3.0 V systému IBM MQ 9.3.0není zahrnut příkaz **fteCreateCDAgent.cmd** . Úplný seznam dostupných příkazů naleznete v tématu Instalované sady příkazů MFT.
- Produkt Managed File TransferConnect:Direct není podporován.
- Položka IBM MQ Explorer není zahrnuta.

Windows Musíte nainstalovat knihovny Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019 , které jsou k dispozici z produktu Microsoft, do svého systému, abyste mohli používat produkt Redistributable Managed File Transfer Agent. Viz Nejnovější podporované soubory ke stažení v jazyce Visual C++.

V 9.3.0 V systému IBM MQ 9.3.0jsou knihovny Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019 také vyžadovány pro Redistributable Managed File Transfer Logger.

Poznámka: Parametr Advanced Message Security není podporován v kombinaci s produktem Redistributable Managed File Transfer package.

Informace o této úloze

Volitelně můžete stáhnout soubor Redistributable Managed File Transfer package a nakonfigurovat server Redistributable Managed File Transfer Agent pro připojení k existující infrastruktuře produktu IBM MQ , abyste umožnili uživatelům přenášet soubory mezi lokálním prostředím a existující infrastrukturou produktu IBM MQ , aniž by museli instalovat produkt IBM MQ , aby získali funkčnost produktu Managed File Transfer .

V 9.3.0 V produktu IBM MQ 9.3.0obsahuje modul Redistributable Managed File Transfer package také modul Redistributable Managed File Transfer Logger, který umožňuje nastavit modul protokolování souborů pro připojení v režimu klienta ke koordinačnímu správci front.

Postup

1. Stáhněte IBM MQ redistribuovatelný Managed File Transfer balík agenta z Fix Central.
   a) Vyberte balík pro váš operační systém.
   Názvy archivních souborů nebo souborů .zip popisují obsah souboru a ekvivalentní úrovně údržby. Názvy souborů jsou v následujícím formátu:
   - Windows *V.R.M.F*-IBM-MQFA-Redist-Win64
   - Linux *V.R.M.F*-IBM-MQFA-Redist-LinuxX64
   - Linux *V.R.M.F*-IBM-MQFA-Redist-LinuxS390X
   - Linux *V.R.M.F*-IBM-MQFA-Redist-LinuxPPC64LE

   kde *V.R.M.F* je číslo verze, například 9.2.0.0 nebo 9.2.1.0.
   b) Identifikujte adresář, do kterého chcete balík extrahovat, například:
   - Windows C:\MFTZ
   - Linux /home/MFTZ
2. Extrahujte obsah staženého balíku:
   - Windows V systému Windowsextrahujte pomocí nástrojů Windows Explorer.
   - Linux V systému Linuxextrahujte a rozbalte následujícím způsobem:

     ```
     gunzip V.R.M.F-IBM-MQFA-Redist-LinuxX64.tar.gz
     ```

     a pak

```
tar xvf V.R.M.F-IBM-MQFA-Redist-LinuxX64.tar
```

kde *V.R.M.F* je číslo verze, například `9.3.0.0` nebo `9.3.1.0`.

Jsou vytvořeny následující adresáře:

- Windows Linux `bin`: Obsahuje všechny požadované příkazy MFT .
- Windows `bin64`: Obsahuje požadované knihovny, které jsou potřebné pro podporu 64bitového operačního systému Windows .
- Windows Linux `java`: Obsahuje knihovny prostředí IBM JRE a IBM MQ .
- Windows Linux `licenses`: Obsahuje soubory s licencemi.
- Windows V 9.3.0 `META-INF`: Obsahuje soubory, které mají informace o podpisu kódu.
- Windows Linux `mqft`: Obsahuje adresáře `ant` a `lib` , které jsou nezbytné pro podporu funkcí Ant a MFT jádra.
- Windows Linux `swtag`: Obsahuje soubor `swidtag` , který správci licencí vyžadují k identifikaci instalací na počítači.

Jak pokračovat dále

Jste připraveni nakonfigurovat Managed File Transfer Agent. Další kroky viz “Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Agent” na stránce 700.

V 9.3.0 V produktu IBM MQ 9.3.0můžete také nakonfigurovat Managed File Transfer Logger. Další kroky konfigurace modulu protokolování viz “Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Logger” na stránce 702.

Související odkazy

Možné chyby při konfiguraci konzoly Redistributable Managed File Transfer components

Windows Linux Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Agent

Můžete nakonfigurovat Managed File Transfer Agent pro připojení k existující konfiguraci produktu IBM MQ .

Než začnete

Ujistěte se, že jste stáhli a extrahovali obsah balíku Redistributable Managed File Transfer Agent . Další informace viz téma “Stažení a konfigurace produktu Redistributable Managed File Transfer components” na stránce 698.

Informace o této úloze

Nejprve vytvoříte prostředí, které produkt Redistributable Managed File Transfer Agent potřebuje. Poté můžete nastavit konektivitu se správcem front, který je spuštěn na serveru IBM MQ , a poté nakonfigurovat agenta a správce front agenta před spuštěním a ověřením agenta.

V 9.3.0 V produktu IBM MQ 9.3.0je prostředí, které vytvoříte, sdíleno s produktem Redistributable Managed File Transfer Logger. Další informace viz téma “Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Logger” na stránce 702.

Postup

1. Vytvořte prostředí pro Redistributable Managed File Transfer Agent.

Když spustíte Příkaz **fteCreateEnvironment**, vytvoří se datový adresář MFT s informacemi o konfiguraci pro agenty MFT . Ujistěte se, že jste v adresáři `bin` , který byl vytvořen při extrahování stažené komponenty Redistributable Managed File Transfer Agent . Spusťte následující příkaz:

- Windows

```
fteCreateEnvironment.cmd -d datapath location
```

- Linux

```
. ./fteCreateEnvironment -d datapath location
```

Tento příkaz má následující volitelné parametry:

-d
Tento parametr určuje umístění cesty k datům, kde je vytvořena, uložena a udržována konfigurace MFT . Spustíte-li příkaz **fteCreateEnvironment** bez určení umístění dat, vytvoří se adresář `mftdata` v umístění, kde je extrahován soubor Redistributable Managed File Transfer Agent .

Poznámka: Pokud bude redistribuovatelný agent spuštěn jako služba Windows , pak musí být proměnná prostředí **BFG_DATA** nastavena v systémovém prostředí, aby mohla tato služba fungovat.

-n *název instalace*
Tento parametr se používá pro zadání názvu instalace produktu IBM MQ nebo jedinečného názvu.

Příklady situací, ve kterých byste mohli chtít použít tento parametr, jsou:

- Chcete-li rychle testovat novou funkci nebo funkci pomocí redistribuovatelného balíku s existující konfigurací, kde byli agenti konfigurováni pro připojení ke správci front pouze v režimu klienta. (Tento parametr se nevztahuje na žádného agenta, který je konfigurován pro připojení ke správci front v režimu vazeb.)
- Pokud provádíte migraci ze standardní instalace produktu Managed File Transfer do balíku Redistributable Managed File Transfer Agent a chcete použít stejnou konfiguraci jako ta, která byla vytvořena standardní instalací. Jedná se o případ, kdy byl nainstalován standardní produkt Managed File Transfer , ale připojuje se ke správci front agenta spuštěnému na jiném počítači.

Výchozí proměnná názvu instalace je **BFG_INSTALLATION_NAME**.

Další informace o příkazu **fteCreateEnvironment** viz fteCreateEnvironment (nastavení prostředí pro Redistributable Managed File Transfer Agent).

Můžete také nastavit proměnnou prostředí *BFG_DATA* s umístěním cesty k datům:

```
BFG_DATA=Datapath location
```

Před vytvořením, spuštěním a zastavením agenta nebo jiných příkazů se musíte ujistit, že je proměnná *BFG_DATA* nastavena na správné umístění cesty k datům.

2. Nastavte konektivitu IBM MQ .
   a) Nastavte koordinačního správce front pomocí příkazu **fteSetupCoordination** .

   Příkaz **fteSetupCoordination** vytvoří sadu, která je nezbytná pro koordinační správce front a adresáře potřebné pro další konfiguraci. Produkt Redistributable Managed File Transfer Agent pracuje v režimu klienta, takže musíte s tímto příkazem zadat další parametry, abyste se vyhnuli chybě, protože režim vazeb není podporován.

```
fteSetupCoordination -coordinationQMgr PRMFTDEMO2
              -coordinationQMgrHost 9.121.59.233 -coordinationQMgrPort 3002
              -coordinationQMgrChannel SYSTEM.DEF.SVRCONN
```

Další podrobnosti a kroky pro použití příkazu **fteSetupCoordination** viz fteSetupCoordination. Informace o konfiguraci koordinačního správce front viz “Konfigurace koordinačního správce front pro MFT” na stránce 741.

b) Vytvořte a nastavte správce front příkazů:

```
fteSetupCommands -p PRMFTDEMO2 -connectionQMgrHost 9.121.59.233
              -connectionQMgrPort 3002 -connectionQMgrChannel SYSTEM.DEF.SVRCONN
              -connectionQMgr PRMFTDEMO2 -f
```

Další podrobnosti a kroky pro použití příkazu **fteSetupCommands** viz fteSetup: vytvořte soubor MFT command.properties.

3. Vytvořte definici agenta MFT pro koncový bod.

```
fteCreateAgent -p PRMFTDEMO2 -agentQMgrHost 9.121.59.233
            -agentQMgrPort 3002 -agentQMgrChannel SYSTEM.DEF.SVRCONN
            -agentName AGENT.TRI.BANK -agentQMgr PRMFTDEMO2 -f
```

Další informace o použití příkazu **fteCreateAgent** ke konfiguraci agenta a správce front agenta viz fteCreateAgent.

Poznámka: K definování objektů agenta ve správci front agenta je třeba použít příkazy MQSC, které jsou zobrazeny jako součást výstupu příkazu, jinak nebudou pokyny v kroku “4” na stránce 702 fungovat.

V krocích “2” na stránce 701 a “3” na stránce 702 pro každého agenta vytvoříte definice front a témat ve správci front agenta.

4. Spusťte agenta a jste připraveni přenést soubory.

```
fteStartAgent -p PRMFTDEMO2 AGENT.TRI.BANK
```

Stav agenta můžete ověřit spuštěním následujícího příkazu:

```
fteListAgents
```

Další podrobnosti o použití příkazu **fteListAgents** viz fteListAgenti.

Jak pokračovat dále

V 9.3.0 Chcete-li konfigurovat server Redistributable Managed File Transfer Logger, postupujte podle pokynů v části “Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Logger” na stránce 702.

Související pojmy

“Konfigurace produktu Managed File Transfer” na stránce 695
Po instalaci můžete nakonfigurovat funkce produktu Managed File Transfer .

“Volby konfigurace MFT na platformě Multiplatforms” na stránce 696
Produkt Managed File Transfer poskytuje sadu souborů vlastností, které obsahují klíčové informace o vašem nastavení a jsou nezbytné pro operaci. Tyto soubory vlastností se nacházejí v konfiguračním adresáři, který jste definovali při instalaci produktu.

Související odkazy

fteCreateTransfer: spuštění nového přenosu souborů

Windows Linux V 9.3.0 Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Logger

Můžete nakonfigurovat typ FILE Managed File Transfer Logger pro připojení ke koordinačnímu správci front v režimu klienta.

Než začnete

Ujistěte se, že jste stáhli a extrahovali obsah balíku Redistributable Managed File Transfer Agent . V produktu IBM MQ 9.3.0tento balík také obsahuje balík Redistributable Managed File Transfer Logger. Další informace viz “Stažení a konfigurace produktu Redistributable Managed File Transfer components” na stránce 698.

Informace o této úloze

Redistributable Managed File Transfer Agent a Redistributable Managed File Transfer Logger sdílejí stejné prostředí. Po vytvoření tohoto prostředí a nastavení konektivity IBM MQ můžete vytvořit a spustit modul protokolování.

Postup

1. Ujistěte se, že bylo vytvořeno sdílené prostředí pro Redistributable Managed File Transfer Agent a Redistributable Managed File Transfer Logger , jak je popsáno v kroku “1” na stránce 700 , a že byla nastavena konektivita IBM MQ , jak je popsáno v kroku “2” na stránce 701 “Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Agent” na stránce 700.

   .
2. Vytvořte modul protokolování souborů pomocí příkazu **fteCreateLogger** .

   Příklad:

   ```
   fteCreateLogger FILELOGGER -loggerType FILE -loggerQMgr PRMFTDEMO2
   -loggerQMgrHost 9.121.59.233 -loggerQMgrPort 3003 -loggerQMgrChannel SYSTEM.DEF.SVRCONN
   -fileSize 20MB -fileCount 10 -fileLoggerMode CIRCULAR
   ```

   Další informace o použití příkazu **fteCreateLogger** viz fteCreateLogger.
3. Spusťte modul protokolování pomocí příkazu **fteStartLogger** .

   Další informace o příkazu **fteStartLogger** viz fteStartLogger.

Související pojmy

“Konfigurace produktu Managed File Transfer” na stránce 695
Po instalaci můžete nakonfigurovat funkce produktu Managed File Transfer .

“Volby konfigurace MFT na platformě Multiplatforms” na stránce 696
Produkt Managed File Transfer poskytuje sadu souborů vlastností, které obsahují klíčové informace o vašem nastavení a jsou nezbytné pro operaci. Tyto soubory vlastností se nacházejí v konfiguračním adresáři, který jste definovali při instalaci produktu.

Windows Linux UpgradováníRedistributable Managed File Transfer components

Produkt Redistributable Managed File Transfer components můžete upgradovat stažením nového souboru Redistributable Managed File Transfer package.

Než začnete

Informace o redistribuovatelných licenčních podmínkách pro Redistributable Managed File Transfer Agent a Redistributable Managed File Transfer Loggernaleznete v tématu IBM MQ Redistribuovatelné komponenty.

Poznámka: Parametr Advanced Message Security není podporován v kombinaci s produktem Redistributable Managed File Transfer package.

Informace o této úloze

Pokud jste již nainstalovali produkt Redistributable Managed File Transfer components, můžete jej upgradovat stažením nového redistribuovatelného balíku a extrahováním obsahu do stejného umístění.

Postup

1. Stáhněte IBM MQ redistribuovatelný Managed File Transfer balík agenta pro váš operační systém z webu Fix Central.
2. Zastavte všechny Managed File Transfer agenty a modul protokolování počkejte na dokončení všech spuštěných příkazů Managed File Transfer .
3. Aktualizujte soubory pro existující instalaci produktu Redistributable Managed File Transfer components extrahováním obsahu nového redistribuovatelného balíku, který jste stáhli do stejného adresáře, jako je adresář, do kterého jste již nainstalovali produkt Redistributable Managed File Transfer components .

z/OS Vytvoření datové sady příkazu MFT Agent nebo Logger

Datovou sadu PDSE příkazů můžete vytvořit z datové sady šablony příkazu Managed File Transfer pro specifickou Managed File Transfer Agent nebo Managed File Transfer Logger pro specifickou koordinaci.

Informace o této úloze

Postupujte takto:

Postup

1. Vytvořte kopii datové sady knihovny PDSE šablony příkazu MFT SCSQFCMD.

   SCSQFCMD musí být zkopírován do nové knihovny, například *prefix.agent*.JCL. Můžete použít aktualizovanou verzi člena SCSQFCMD (BFGCOPY) s následujícími náhradami:

   - Nahraďte *+ + dodaná knihovna + +* úplným názvem SCSQFCMD PDSE.
   - z/OS Řetězec *+ + service-library + +* nahraďte úplným názvem nové datové sady knihovny PDSE příkazu MFT . *+ + knihovna služeb + +* je výstupní datová sada pro vytvořeného agenta nebo službu modulu protokolování.
2. Pro novou datovou sadu knihovny PDSE příkazu MFT upravte člena BFGCUSTM, což je skript JCL, který upravuje příkazy pro agenta nebo modul protokolování. Každá proměnná je určena ve formátu: *+ + název proměnné + +*, který musíte nahradit požadovanou hodnotou. Popis různých proměnných JCL viz “z/OS proměnné JCL” na stránce 716. Příkaz BFGSTDIN DD definuje proměnné ve třech kategoriích: Proměnné, Vlastnosti a Prostředí. Příkaz má následující formát:

   ```
   [Variables]
   variable1=value1
   variable2=value2
   ....
   variableN=valueN
   [Properties]
   property1=property value1
   property2=property value2
   ...
   propertyN=property valueN
   [Environment]
   custom_variable1=value1
   custom_variable2=value2
   ....
   custom_variableN=valueN
   ```

   Proměnné definují sadu proměnných nastavení a prostředí, které jsou vyžadovány pro každý příkaz.

   Vlastnosti definují přepisy pro vlastnosti konfigurace MFT . Podle potřeby můžete přidat vlastnosti agenta a modulu protokolování, chcete-li upravit agenta nebo modul protokolování pro své prostředí. Seznam všech vlastností viz “Soubory vlastností konfigurace” na stránce 726. Tento prostředek je poskytován pro uložení nutnosti přístupu k souborům vlastností konfigurace MFT , které jsou udržovány jako soubory z/OS UNIX System Services .

   Prostředí definuje všechny dodatečně požadované vlastní proměnné prostředí.

3. Zadejte úlohu BFGCUSTM pro novou datovou sadu knihovny PDSE příkazu MFT . Tato úloha vygeneruje sadu příkazů JCL jako nové členy PDSE odpovídající agentovi nebo modulu protokolování. Úplný seznam příkazů naleznete v části “Skripty JCL agenta a příkazu modulu protokolování z/OS” na stránce 719.

   Úloha BFGCUSTM aktualizuje knihovnu obsahující JCL, který obsahuje příkaz DD s DISP=OLD. Chcete-li povolit provedení úlohy, musíte po odeslání ukončit editor.

   Zkontrolujte výstupní protokol úlohy a zkontrolujte, zda skript JCL proběhl úspěšně. Pokud dojde k selhání, opravte je a znovu zadejte úlohu BFGCUSTM.

   Skript BFGCUSTM JCL také aktualizuje soubory vlastností konfigurace produktu z/OS UNIX System Services MFT podle potřeby, aby uchovávaly soubory v kroku. Pokud konfigurace definovaná vlastností CoordinationQMgr neexistuje, jsou výstupní varovné zprávy a musíte spustit generované úlohy BFGCFCR a BFGCMCR, abyste vytvořili soubory vlastností konfigurace. Musíte spustit BFGAGCR pro agenta a BFGLGCRS pro úpravu modulu protokolování. Pokud zadaná konfigurace již existuje, je aktualizována o všechny vlastnosti definované ve skriptu BFTCUSTM JCL.

Související pojmy

“MFT volby konfigurace na z/OS” na stránce 697
Volby konfigurace Managed File Transfer v systému z/OS jsou stejné jako volby pro distribuované platformy.

Související úlohy

“Aktualizace existující datové sady příkazu MFT Agent nebo Logger na systému z/OS” na stránce 715
Můžete aktualizovat datovou sadu knihovny PDSE příkazu Managed File Transfer , která je vytvořena z datové sady šablony příkazu Managed File Transfer .

z/OS Konfigurace produktu Managed File Transfer for z/OS

Produkt Managed File Transfer for z/OS vyžaduje přizpůsobení, aby komponenta mohla správně fungovat.

Informace o této úloze

Musíte provést následující akce:

1. Upravit člena PDSE tak, aby uváděli konfigurační data
2. Definujte koordinačního správce front.
3. Definovat správce front příkazů
4. Konfigurovat jednoho nebo více agentů
5. Volitelně: nakonfigurujte úlohu modulu protokolování pro ukládání dat v produktu Db2

Posloupnost úloh, které je třeba provést, je podrobně popsána v následujících tématech.

Související pojmy

“Přezkoumání konfigurace MFT” na stránce 705
Než začnete, musíte zkontrolovat konfiguraci systému.

Související úlohy

Instalace produktu IBM MQ Advanced for z/OS

z/OS Přezkoumání konfigurace MFT

Než začnete, musíte zkontrolovat konfiguraci systému.

Managed File Transfer (MFT) vyžaduje, aby jeden nebo více správců front pracovaly v následujících rolích pro každou definovanou konfiguraci MFT:

- Koordinační správce front, který udržuje informace o stavu jednotlivých agentů v konfiguraci publikované v tématu koordinátora.

- Jeden nebo více správců front příkazů nebo připojení, kteří slouží jako vstupní bod do sítě IBM MQ pro příkazy MFT.
- Jeden nebo více správců front agenta, kteří poskytují komunikaci mezi agentem MFT a sítí IBM MQ .

Každou z výše uvedených rolí může provádět samostatný správce front nebo můžete tyto role kombinovat tak, aby v nejjednodušší konfiguraci byly všechny role prováděny jedním správcem front.

Pokud přidáváte správce front z/OS do existujícího prostředí MFT, musíte definovat konektivitu mezi správcem front z/OS a ostatními správci front v konfiguraci. Toho lze dosáhnout pomocí ručně definovaných přenosových front nebo pomocí klastrování.

Každý agent MFT komunikuje s jedním správcem front. Pokud se stejným správcem front komunikuje více agentů, bude mít správce front agenta definováno více front pro každého agenta:

- SYSTEM.FTE.COMMAND.*název_agenta*
- SYSTEM.FTE.DATA.*název_agenta*
- SYSTEM.FTE.REPLY.*název_agenta*
- SYSTEM.FTE.STATE.*název_agenta*
- SYSTEM.FTE.EVENT.*název_agenta*
- SYSTEM.FTE.AUTHAGT1.*název_agenta*
- SYSTEM.FTE.AUTHTRN1.*název_agenta*
- SYSTEM.FTE.AUTHOPS1.*název_agenta*
- SYSTEM.FTE.AUTHSCH1.*název_agenta*
- SYSTEM.FTE.AUTHMON1.*název_agenta*
- SYSTEM.FTE.AUTHADM1.*název_agenta*

Všimněte si, že můžete definovat generické profily zabezpečení, kde použijete profil, jako např. `SYSTEM.FTE.COMMAND.*`, nebo můžete definovat specifické profily pro každého agenta.

Související pojmy

“Než začnete konfigurovat MFT pro z/OS” na stránce 706

Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách z/OS UNIX System Services (z/OS UNIX) a PDSE.

Související odkazy

Systémové fronty MFT a téma systému

z/OS Než začnete konfigurovat MFT pro z/OS

Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách z/OS UNIX System Services (z/OS UNIX) a PDSE.

Většina konfigurace a operace se provádí pomocí JCL z PDSE a musíte být obeznámeni s prací v prostředí z/OS UNIX .

K OMVS můžete přistupovat z ISPF nebo můžete použít relaci typu Telnet pomocí příkazů na pracovní stanici, například Telnet Putty nebo SSH.

Pokud používáte OMVS z ISPF , můžete použít standardní ISPF a příkazy procházení **oedit** a **obrowse**.

Musíte se seznámit s následujícími příkazy z/OS UNIX

Tabulka 40. Běžné příkazy z/OS UNIX

Příkaz	**Funkce**
chmod xxx cesta	Změňte přístupová oprávnění k souborům.
df -k cesta	Uvádí, kolik volného prostoru zbývá v systému souborů. -k uvádí volné místo v kB.

Tabulka 40. Běžné příkazy z/OS UNIX (pokračování)	
Příkaz	**Funkce**
du -kt cesta	Uvádí velikost adresářů v cestě. Velikost hlášená v kB.
najít cestu -name xxx	Vyhledejte soubor s názvem `xxxx` v adresáři cesty. xxx rozlišuje velikost písmen a může být jako `*zzz`.
ls -ltrd adresář	Vypíše informace o uvedeném adresáři spíše než o souborech v adresáři.
ls -ltr cesta	Vypíše informace o souborech v cestě.
název souboru obrowse	Procházejte název souboru.
název souboru oedit	Upravte soubor v OMVS.

Přezkoumejte položky v následující tabulce a dokončete tabulku s odpovídajícími položkami pro váš podnik. Tyto hodnoty potřebujete při úpravě členu BFGCUSTM.

Tabulka 41. Parametry potřebné pro člen BFGCUSTM		
Název	**Příklad dat**	**Komentář**
ADMIN_JOB1		Zakázkový list. Všechny úlohy jsou generovány se stejnou kartou JCL.
armELEMENT	Pokud se používá ARM, použijte hodnotu ARM ELEMENT uvedenou v zásadě ARM pro tohoto agenta nebo modul protokolování. Pokud se nepoužívá ARM, nastavte tento parametr na prázdnou hodnotu; například armELEMENT=	
armELEMTYPE	Pokud se používá ARM, použijte ARM ELEMTYPE uvedený v zásadě ARM. Například armELEMTYPE= SYSBFGAG pro agenta nebo armELEMTYPE= SYSBFGLG pro modul protokolování. Pokud se nepoužívá ARM, nastavte tento parametr na prázdnou hodnotu; například armELEMTYPE=	
BFG_DATA		Dokončit podle potřeby
NÁZEV_SKUPINY_BFG_	MQM	
BFG_JAVA_HOME	`/java/java71_bit64_GA/J7.1_64/`	
VLASTNOSTI BFG_JVM_PROPERTIES		Dokončit podle potřeby
BFG_PROD	`/mqm/V9R2M0/mqft`	Úplná cesta k adresáři `mqft` v adresáři IBM MQ for z/OS UNIX System Services Components .
BFG_WTO	YES	Chcete-li získat zprávu MFT na syslog.

Tabulka 41. Parametry potřebné pro člen BFGCUSTM (pokračování)		
Název	**Příklad dat**	**Komentář**
PROPS příkazu CLEAN_AGENT_PROPS	-trs	Tento parametr určuje volby, které se použijí k vyčištění agenta při spuštění člena BFGAGCL. Další informace o platných hodnotách tohoto parametru naleznete v tématu fteCleanAgent: vyčištění MFT agenta.
coordinationQMgr	MQPV	Povinná konfigurace
CESTA_K_POVĚŘENÍ		Používá se při migraci
Db2_HLQ	SYS2.Db2.V10	
DB_PROPS_PATH		Používá se při migraci
FTE_CONFIG		Používá se při migraci
JOBCARD1		Jedná se o zakázkový list pro dlouhodobě spuštěné úlohy, agenty a zapisovače protokolu.
KNIHOVNA	SCEN.FTE.JCL	Název MFT PDSE. Potřebujete kopii pro každého agenta nebo úlohu modulu protokolování.
MQ_HLQ	Kvalifikátor vyšší úrovně pro datové sady IBM MQ . Například: `MQM.V920`	
MQ_LANG	E	
MQ_PATH	`/mqm/V9R2M0`	Úplná cesta k adresáři instalace produktu IBM MQ for z/OS UNIX System Services Components.
NÁZEV	AGENT1	
VÝSTUPNÍ_TŘÍDA	*	
Cesta	`bin:/usr/bin:/usr/sbin`	
productId	ADVANCEDVUE	Tento parametr se používá k nastavení typu produktu, pro který má být zaznamenáno využití produktu Managed File Transfer . Informace o platných hodnotách pro tento parametr viz fteSetProductId: set z/OS SCRT recording product id.
QMGR	MQPV	
SERVICE_TYPE-TYP služby	AGENT nebo LOGGER	
TMPDIR	`/tmp`	Cesta k dočasným souborům, která je přístupná pro čtení a zápis, z/OS UNIX .

Kromě toho musíte zkontrolovat následující proměnné a v případě potřeby zadat hodnoty:

- coordinationQMgrHostitel =

- coordinationQMgrPort =
- coordinationQMgrKanál =
- connectionQMgr=
- connectionQMgrHostitel =
- connectionQMgrPort =
- connectionQMgrKanál =

Tyto vlastnosti jsou společné pro AGENT nebo LOGGER.

Poznámka: Hostitel, port a kanál jsou vyžadovány pro připojení klienta, ale pro připojení vazeb v lokálním počítači by měly zůstat prázdné.

Související pojmy

"Položky ke kontrole" na stránce 709
Ujistěte se, že máte dostatek místa na disku, adresář pro ukládání dat a že požadované soubory existují.

"Úprava člena BFGCUSTM" na stránce 711
Před spuštěním úlohy musíte upravit člena BFGCUSTM a zadat hodnoty parametrů, které váš podnik používá.

z/OS Položky ke kontrole

Ujistěte se, že máte dostatek místa na disku, adresář pro ukládání dat a že požadované soubory existují.

Zkontrolujte, zda máte dostatek místa na disku

Zkontrolujte, zda máte dostatek volného místa na disku v systému souborů, kde budete ukládat soubory specifické pro konfiguraci.

Pokud je trasování agenta povoleno, může standardně použít 100 MB místa na disku.

Samotné konfigurační soubory jsou malé, velikost je jen několik kB.

Pokud plánujete použití dvou agentů a modulu protokolování, pak potřebujete alespoň 300 MB. Můžete použít příkaz **df -k** `path`, kde `path` je umístění souborů specifických pro instalaci. Poskytuje dostupný a celkový prostor v kB.

300 MB je 307 200 KB, takže byste měli povolit alespoň 310 000 KB

Vytvořte a zkontrolujte adresář pro ukládání dat Managed File Transfer

Potřebujete adresář pro ukládání dat Managed File Transfer (MFT).

Zkontrolujte, zda máte v systému souborů `df -k /var`dostatek místa. Tento systém souborů by měl mít k dispozici alespoň 10000 kB.

Pokud jste tento systém souborů nevytvořili, použijte příkaz **mkdir** , například **mkdir /var/mft**.

Zobrazte, jaká oprávnění mají uživatelé k tomuto adresáři, pomocí příkazu **ls -ltrd /var/mft**.

Pokud vlastník nebo skupina nejsou správné, použijte příkaz **chown owner:group /var/mft**.

Pokud nejsou oprávnění pro skupinu správná, pomocí následujícího příkazu udělte vlastníkovi a skupině oprávnění ke čtení, zápisu a provádění. Všimněte si, že následující příkaz také uděluje všem uživatelům oprávnění ke čtení a provádění **chmod 775 /var/mft**.

Zkontrolujte, zda soubory existují a zda k nim máte přístup.

Použijte příkaz **ls -ltr** pro soubory, které budete používat během přizpůsobení. Příklad:

```
ls -ltrd /java/java71_bit64_GA/J7.1_64/bin
```

dává

```
drwxr-xr-x  4 SYSTASK TSOUSER   8192 Nov 15 2013 /java/java71_bit64_GA/J7.1_64/bin
```

kde `drwxr-xr-x` znamená,

d
Toto je adresář.

rwx
Vlastník *SYSTASK* má k adresáři přístup pro čtení, zápis a provádění.

r-x
Uživatelé ve skupině *TSOUSER* mohou číst a spouštět soubory v adresáři.

r-x
Univerzální přístup, to znamená, že kdokoli může číst nebo spouštět soubory v adresáři.

Zkontrolujte soubory uvedené v:

Tabulka 42. Přístup vyžadovaný uživateli ke specifickým souborům

Cesta	**Přístup požadovaný uživateli, který provádí konfiguraci**
BFG_JAVA_HOME	Čtení a provádění
/tmp	Čtení a zápis
BFG_PROD	Číst
BFG_DATA	Zapisovat
MQ_PATH	Číst

Související pojmy

“Než začnete konfigurovat MFT pro z/OS” na stránce 706
Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách z/OS UNIX System Services (z/OS UNIX) a PDSE.

“Společná konfigurace MFT pro z/OS” na stránce 710
Přehled různých konfigurací produktu Managed File Transfer

z/OS Společná konfigurace MFT pro z/OS

Přehled různých konfigurací produktu Managed File Transfer

Produkt Managed File Transfer používá pro přenos dat agenty připojené ke správci front.

MFT může používat více správců front:

- Jeden nebo více správců front pro přenos dat.
- Správce front příkazů, který vydává požadavky. Například požadavek na zahájení přenosu se odešle na tohoto správce front a na agenty MFT se přesměrují přidružené příkazy.
- Koordinační správce front, který spravuje práci.

Existují tři běžné konfigurace Managed File Transfer (MFT):

1. Jeden správce front s jedním nebo více agenty používající lokální připojení. Tuto konfiguraci lze použít ke vkládání obsahu datové sady do front produktu IBM MQ.
2. Jeden správce front s klientem MFT na distribuovaném počítači používající vazby klienta.
3. Dva správci front propojené kanály a jeden nebo více agentů na každém počítači. Tito agenti mohou být klienty nebo lokálními vazbami.

Všimněte si následujících bodů:

1. MFT je napsán v jazyce Java spolu s některými skripty shellu a jazyce JCL pro konfiguraci a provoz MFT.
2. Stav a aktivita databáze Db2 může být protokolována a tyto informace lze ukládat do tabulek Db2.
3. Osoba, která konfiguruje MFT, musí být obeznámena s z/OS UNIX System Services (z/OS UNIX). Například:
   - Adresářová struktura se soubory, které mají názvy jako `/u/userID/myfile.txt2`
   - Příkazy z/OS UNIX, např.:

     cd (změna adresáře)
     ls (seznam)
     chmod (změna oprávnění souboru)
     chown (změna vlastnictví souboru nebo skupin, které mohou přistupovat k souboru nebo adresáři)
4. Následující produkty jsou v z/OS UNIX nezbytné, aby bylo možné nakonfigurovat a provozovat MFT:
   - Java; například `/java/java71_bit64_GA/J7.1_64/`
   - IBM MQ V920, například `/mqm/V9R2M0`.
   - Knihovny JDBC Db2, pokud chcete použít Db2 pro stav a historii, například `/db2/db2v12/jdbc/lib`

Potřebujete koordinačního správce front. Stejného správce front však můžete použít ke spuštění agentů, ke zpracování příkazů a ke koordinaci. Používáte-li více správců front, musíte vybrat jednoho, který bude fungovat jako koordinátor.

Zkontrolujte IBM MQ konektivitu

Máte-li existujícího správce front koordinátora MFT , potřebujete konektivitu mezi správcem front, kde provádíte konfiguraci, a koordinačními a příkazovými správci front.

z/OS Kopírovat SCSQFCMD pro vytvoření knihovny JCL

Musíte vytvořit knihovnu JCL pro každého agenta a modul protokolování. JCL obsahuje konfiguraci a úlohy použité k vytvoření a spuštění agenta nebo modulu protokolování.

Pro každého agenta a modul protokolování vytvořte kopii knihovny SCSQFCMD dodané produktem IBM úpravou a spuštěním člena BFGCOPY.

Tato knihovna se používá k definování konfigurace agenta nebo modulu protokolování a po přizpůsobení obsahuje úlohy, které lze použít k vytvoření požadované konfigurace produktu Managed File Transfer a agenta nebo modulu protokolování.

Jako součást tohoto procesu vytvoříte člena BFGCUSTM.

Poznámka: Pokud jste obeznámeni s příkazy z/OS UNIX , můžete nakonfigurovat produkt z/OS pomocí stejných příkazů, které používáte na jiných platformách.

Související pojmy

“Společná konfigurace MFT pro z/OS” na stránce 710
Přehled různých konfigurací produktu Managed File Transfer

“Úprava člena BFGCUSTM” na stránce 711
Před spuštěním úlohy musíte upravit člena BFGCUSTM a zadat hodnoty parametrů, které váš podnik používá.

z/OS Úprava člena BFGCUSTM

Před spuštěním úlohy musíte upravit člena BFGCUSTM a zadat hodnoty parametrů, které váš podnik používá.

Viz Parametry potřebné pro člen BFGCUSTM, kde je seznam parametrů vyžadujících specifické hodnoty.

Kromě toho musíte zkontrolovat následující proměnné a v případě potřeby zadat hodnoty:

- coordinationQMgrHostitel =
- coordinationQMgrPort =
- coordinationQMgrKanál =
- connectionQMgr=
- connectionQMgrHostitel =
- connectionQMgrPort =
- connectionQMgrKanál =

Tyto vlastnosti jsou společné pro AGENT nebo LOGGER.

Poznámka: Hostitel, port a kanál jsou vyžadovány pro připojení klienta, ale pro připojení vazeb v lokálním počítači by měly zůstat prázdné.

Pokud se jedná o prvního správce front ve vašem prostředí Managed File Transfer a chcete použít stejného správce front pro koordinaci, příkazy a spuštěné agenty, nastavte hodnoty na název lokálního správce front.

```
coordinationQMgr=MQPV
connectionQMgr=MQPV
```

kde MQPV je název lokálního správce front.

Odešlete úlohu, která aktualizuje PDSE, a vytvoří adresářovou strukturu pod uvedenou cestou.

Všimněte si, že tato úloha vyžaduje výlučné použití, takže musíte přestat používat PSDE, když je úloha spuštěna.

Rada: Kdykoli odešlete úlohu BFGCUSTM, úloha nahradí všechny soubory JCL. Měli byste přejmenovat každého člena, kterého změníte.

Související pojmy

“Než začnete konfigurovat MFT pro z/OS” na stránce 706
Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách z/OS UNIX System Services (z/OS UNIX) a PDSE.

“Vytvoření agenta” na stránce 714
Musíte zkopírovat PDSE, abyste učinili PDSE specifickou pro agenta, například *user.MFT.AGENT1*. Zkopírujte PDSE z předchozího agenta nebo konfigurace modulu protokolování, pokud existují. Pokud se jedná o první konfiguraci, zkopírujte PDSE dodávanou s MFT.

z/OS Definování koordinačního správce front

Produkt Managed File Transfer vyžaduje vytvoření správce front, který bude fungovat jako koordinační správce front.

V závislosti na vybrané konfiguraci se tento správce front nachází v lokálním systému MVS nebo v jiném počítači. V prvním případě se jedná o připojení vazeb a v druhém případě se jedná o připojení klienta.

Po úspěšném spuštění kroku konfigurace jsou v PDSE nakonfigurovaní členové.

Člen BFGCFCR definuje koordinačního správce front a tuto úlohu:

1. Vytvoří adresářovou strukturu v adresáři Managed File Transfer (MFT) a vytvoří konfigurační soubory.
2. Spouští CSQUTIL pro definování prostředků IBM MQ .

Pokud se koordinační správce front nachází na vzdáleném počítači, tento krok úlohy se nezdaří.

Člen BCFCFCR vytváří soubory v produktu z/OS UNIX System Services a vytváří definice produktu MQ . Toto pracovní místo:

1. Vytvoří téma MFT,
2. Vytvoří frontu MFT

3. Změní seznam *NAMELIST (SYSTEM.QPUBSUB.QUEUE.NAMELIST)* bude mít hodnotu *NAMES (SYSTEM.BROKER.DEFAULT.STREAM, SYSTEM.BROKER.ADMIN.STREAM, SYSTEM.FTE)*
4. Provede příkaz *ALTER QMGR PSMODE (ENABLED)*

   DISPLAY NAMELIST (SYSTEM.QPUBSUB.QUEUE.NAMELIST) . Pokud váš parametr NAMLIST není výchozí, měli byste změnit seznam jmen a přidat systém SYSTEM.FTE do vašeho seznamu názvů

Přejmenujte člen BCFCFCR s vlastní předponou, například CCPCFCR, protože jej znovu upravte tímto souborem.

Upravte tento přejmenovaný člen vložením názvu souboru pověření. Příklad:

```
%BFGCMD CMD=fteSetupCoordination +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>'
```

Uložte a odešlete úlohu. Všimněte si, že pokud potřebujete úlohu znovu odeslat, musíte přidat volbu *-f* .

Když se tato úloha spustí, vypíše se seznam prostředků IBM MQ , které vytvoří. Tyto prostředky musíte chránit.

```
DEFINE TOPIC('SYSTEM.FTE') TOPICSTR('SYSTEM.FTE') REPLACE
ALTER TOPIC('SYSTEM.FTE') NPMSGDLV(ALLAVAIL) PMSGDLV(ALLAVAIL)
DEFINE QLOCAL(SYSTEM.FTE) LIKE(SYSTEM.BROKER.DEFAULT.STREAM) REPLACE
ALTER QLOCAL(SYSTEM.FTE) DESCR('Stream for MFT Pub/Sub interface')
* Altering namelist: SYSTEM.QPUBSUB.QUEUE.NAMELIST
* Value prior to alteration:
DISPLAY NAMELIST(SYSTEM.QPUBSUB.QUEUE.NAMELIST)
ALTER NAMELIST(SYSTEM.QPUBSUB.QUEUE.NAMELIST) +
NAMES(SYSTEM.BROKER.DEFAULT.STREAM+
,SYSTEM.BROKER.ADMIN.STREAM,SYSTEM.FTE)
* Altering PSMODE. Value prior to alteration:
DISPLAY QMGR PSMODE
ALTER QMGR PSMODE(ENABLED)
```

Související úlohy

“Definování správce front příkazů” na stránce 713
Můžete buď použít stejného správce front jako koordinační správce front a správce front příkazů, nebo vytvořit nového správce front příkazů.

z/OS Definování správce front příkazů

Můžete buď použít stejného správce front jako koordinační správce front a správce front příkazů, nebo vytvořit nového správce front příkazů.

Informace o této úloze

Musíte mít správce front příkazů, ale můžete použít stejného správce front pro koordinaci a správce front příkazů. V opačném případě je třeba vytvořit nového správce front příkazů. Může se nacházet ve stejném počítači jako koordinační správce front, ale nemusí být.

Postup

1. Přejmenujte člen BFGCMCR s vlastní předponou, například CCPCMCR.

   Musíte přejmenovat BFGCMCR, protože jeho opětovné přizpůsobení nahradí tento soubor.
2. Upravte přejmenovaný člen vložením názvu svého souboru pověření.

   Příklad:

   ```
   %BFGCMD CMD=fteSetupCommands +
   -credentialsFile //'<MFTCredentialsDataSet(MemberName)>' +
   ```
3. Uložte a odešlete úlohu.

   Všimněte si, že pokud potřebujete úlohu znovu odeslat, musíte přidat volbu *-f* .

Tento správce front se používá pro příkazy, jako např. **ftePingAgent**.

4. Zkontrolujte tohoto člena, odešlete jej a přezkoumejte výstup.

Jak pokračovat dále

Informace o tom, jak vytvořit agenta, viz “Vytvoření agenta” na stránce 714 .

Související pojmy

“Definování koordinačního správce front” na stránce 712
Produkt Managed File Transfer vyžaduje vytvoření správce front, který bude fungovat jako koordinační správce front.

Související úlohy

Konfigurace souboru MQMFTCredentials.xml

Související odkazy

Formát souboru pověření MFT

z/OS Vytvoření agenta

Musíte zkopírovat PDSE, abyste učinili PDSE specifickou pro agenta, například *user.MFT.AGENT1*. Zkopírujte PDSE z předchozího agenta nebo konfigurace modulu protokolování, pokud existují. Pokud se jedná o první konfiguraci, zkopírujte PDSE dodávanou s MFT.

Zkontrolujte člen BFGCUSTM a pokud potřebujete použít jiný soubor pověření, vytvořte jej.

Velká část obsahu zůstává stejná z přizpůsobení, které je podrobně popsáno v tématu “Úprava člena BFGCUSTM” na stránce 711.

Musíte změnit:

- // SYSEXEC DD DSN=SCEN.FTE.JCL.AGENT1
- KNIHOVNA pro shodu s agentem PDSE
- TYP_SLUŽBY=AGENT
- NAME jako název agenta (odpovídající PDSE) JOBCARD
- Změna BFG_JVM_PROPERTIES = "-Xmx1024M"

Odešlete tuto úlohu s tím, že úloha vyžaduje výlučný přístup k datové sadě.

Všechny úlohy pro agenta mají názvy ve tvaru *BFGAG**

Přejmenujte člena *BFGAGCR*. Tato úloha aktualizuje soubory v adresáři Managed File Transfer a používá CSQUTIL k vytvoření front specifických pro agenta v lokálním správci front. Zadejte název souboru pověření, například `-credentialsFile //'SCEN.FTE.JCL.VB(CREDOLD)`. Pokud neuvedete název, úloha pro spuštění agenta nebude používat soubor pověření.

Zkontrolujte výstup a ujistěte se, že proces proběhl úspěšně.

Rada: Zkopírujte název cesty souboru *agent.properties* z výstupu úlohy na člena v PDSE pro agenta.

Například zkopírujte soubor `/u/userid/fte/wmqmft/mqft/config/MQPA/agents/AGENT1/agent.properties` do člena AGENT.

To je užitečné, pokud potřebujete zobrazit soubor vlastností a přidat řádek `/u/userid/fte/wmqmft/mqft/logs/MQPA/agents/AGENT1/logs`.

Zde jsou uloženy trasovací soubory.

Související pojmy

“Definování koordinačního správce front” na stránce 712
Produkt Managed File Transfer vyžaduje vytvoření správce front, který bude fungovat jako koordinační správce front.

“Použití agenta” na stránce 715

Jak použijete různé příkazy, abyste se ujistili, že agent pracuje správně.

Související úlohy

“Definování správce front příkazů” na stránce 713
Můžete buď použít stejného správce front jako koordinační správce front a správce front příkazů, nebo vytvořit nového správce front příkazů.

z/OS Použití agenta

Jak použijete různé příkazy, abyste se ujistili, že agent pracuje správně.

Spuštění agenta

Přejmenujte člena BFGAGST, přezkoumejte člena a odešlete úlohu.

Pokud to funguje, obdržíte zprávu BFGAG0059I: Agent byl úspěšně spuštěn.

Zobrazit aktivní agenty

Přejmenujte člena BFGAGLI, zkontrolujte člena a odešlete úlohu, která používá koordinačního správce front.

Je třeba vyřešit případné problémy s konektivitou.

Testování spojení s agentem, aby se ověřilo, že pracuje

Přejmenujte člena BFGAGPI, zkontrolujte člena a odešlete úlohu, která používá správce front příkazů.

Je třeba vyřešit případné problémy s konektivitou.

Provést testovací přenos

Další informace viz “Provedení přenosu ověření” na stránce 721.

Zastavení agenta

Přejmenujte člena BFGAGSP, přezkoumejte člena a odešlete úlohu.

Restartujte agenta pomocí člena BFGAGST.

Související pojmy

“Vytvoření agenta” na stránce 714
Musíte zkopírovat PDSE, abyste učinili PDSE specifickou pro agenta, například *user.MFT.AGENT1*. Zkopírujte PDSE z předchozího agenta nebo konfigurace modulu protokolování, pokud existují. Pokud se jedná o první konfiguraci, zkopírujte PDSE dodávanou s MFT.

z/OS Aktualizace existující datové sady příkazu MFT Agent nebo Logger na systému z/OS

Můžete aktualizovat datovou sadu knihovny PDSE příkazu Managed File Transfer , která je vytvořena z datové sady šablony příkazu Managed File Transfer .

Postup

1. Upravte člena skriptu BFGCUSTM JCL a aktualizujte proměnné a vlastnosti v příkazu BFGSTDIN DD.

   Chcete-li odebrat vlastnost, která byla dříve definována, nastavte její hodnotu na prázdnou, namísto odebrání položky. Při spuštění skriptu JCL BFGCUSTM se zadané vlastnosti použijí jako aktualizace skutečných souborů vlastností agenta a modulu protokolování z/OS UNIX System Services ; nastavení vlastnosti na prázdnou hodnotu označuje, že vlastnost má být odebrána.

2. Zadejte úlohu BFGCUSTM. Tato úloha znovu vygeneruje sadu příkazů JCL, která je vhodná pro agenta nebo modul protokolování. Úplný seznam příkazů naleznete v části “Skripty JCL agenta a příkazu modulu protokolování z/OS” na stránce 719. Zkontrolujte výstupní protokol úlohy a zkontrolujte, zda skript JCL proběhl úspěšně. Pokud dojde k selhání, opravte je a znovu zadejte úlohu BFGCUSTM.

Výsledky

Můžete upravit vygenerované skripty JCL a přidat vlastní logiku. Buďte však opatrní, když znovu spustíte BFGCUSTM, protože byste mohli přepsat vlastní logiku.

Související pojmy

“MFT volby konfigurace na z/OS” na stránce 697
Volby konfigurace Managed File Transfer v systému z/OS jsou stejné jako volby pro distribuované platformy.

Související úlohy

“Vytvoření datové sady příkazu MFT Agent nebo Logger” na stránce 704
Datovou sadu PDSE příkazů můžete vytvořit z datové sady šablony příkazu Managed File Transfer pro specifickou Managed File Transfer Agent nebo Managed File Transfer Logger pro specifickou koordinaci.

z/OS *z/OS proměnné JCL*

Ve skriptu BFGCUSTM můžete použít substituční hodnoty, proměnné JCL a konfigurační vlastnosti.

V následující tabulce jsou uvedeny substituční hodnoty pro skript BFGCUSTM JCL v datové sadě knihovny PDSE příkazu MFT . Před odesláním úlohy BFGCUSTM musíte tyto substituční hodnoty nahradit vhodnými hodnotami.

Tabulka 43. Substituční hodnoty pro skript BFGCUSTM JCL

Substituční proměnná	**Hodnota**
+ + knihovna + +	Název datové sady obsahující knihovny PDSE příkazu MFT .
+ + bfg_java_home + +	Umístění instalace produktu Java .
+ + mq_path + +	Cesta k adresáři IBM MQ for z/OS UNIX System Services Components . Například `/mqm/V9R2M0`. Používá se k zadání úplné cesty k instalaci produktu MFT , například `/mqm/V9R2M0/mqft`.

Následující tabulka popisuje proměnné prostředí pro příkaz BFGSTDIN DD pro skript BFGCUSTM JCL v datové sadě knihovny PDSE příkazu MFT (v sekci [Proměnné]). Před odesláním úlohy BFGCUSTM musíte nahradit všechny proměnné, které jsou uvedeny, substitučními hodnotami (tj. hodnotami uzavřenými dvěma znaménky plus, + +) vhodnými hodnotami.

Tabulka 44. Proměnné prostředí

Proměnná prostředí	**Hodnota**
KNIHOVNA	Název datové sady obsahující knihovny PDSE příkazu MFT .
TMPDIR	Adresář z/OS UNIX System Services pro dočasné soubory.
BFG_PROD	Úplná cesta k adresáři `mqft` v adresáři IBM MQ for z/OS UNIX System Services Components ; například: `/mqm/V9R2M0/mqft`.
BFG_DATA	Umístění datového adresáře Managed File Transfer pro z/OS, což je cesta k adresáři *DATA_DIR*.
BFG_JAVA_HOME	Umístění instalace produktu Java .

Tabulka 44. Proměnné prostředí (pokračování)	
Proměnná prostředí	**Hodnota**
VLASTNOSTI BFG_JVM_PROPERTIES	Volitelné. Nastaví hodnotu pro proměnnou prostředí BFG_JVM_PROPERTIES. Tyto vlastnosti jsou předány virtuálnímu počítači Java .
NÁZEV_SKUPINY_BFG_	Skupina souborů mqm je obvykle přidružena k souborům a příkazům konfiguračních dat MFT . V důsledku toho mohou všichni uživatelé, kteří jsou členy skupiny mqm, přistupovat ke konfiguraci MFT a provádět její změny. Další informace viz Oprávnění systému souborů pro MFT v části IBM MQ. Pro systém z/OS je skupina souborů entitou systému souborů z/OS UNIX System Services (z/OS UNIX) a skupina souborů mqm není nutně definována. Skupinu systémů souborů z/OS UNIX pro soubory konfiguračních dat MFT můžete přidružit pomocí proměnné prostředí BFG_GROUP_NAME. Například na příkazovém řádku shellu z/OS UNIX použijte: `export BFG_GROUP_NAME=FTEGB` který definuje skupinu *FTEGB* , která má být přidružena k libovolným následně vytvořeným konfiguračním souborům pro aktuální relaci z/OS UNIX . Parametr BFG_GROUP_NAME můžete nastavit na prázdnou hodnotu nebo jej můžete odebrat. **Poznámka:** Při prvním spuštění BFGCUSTM, pokud má být konfigurace MFT používána více ID uživatelů, je důležité, aby byl parametr BFG_GROUP_NAME nastaven na skupinu přístupnou všem požadovaným ID uživatele. Pokud je BFGCUSTM spuštěn znovu, pak BFG_GROUP_NAME nesmí být změněn (jinak musí být oprávnění skupinového souboru z/OS UNIX pro všechny soubory a adresáře v adresáři, na který odkazuje BFG_DATA, také změněna, aby odrážela nové nastavení BFG_GROUP_NAME).
BFG_WTO	Protokolování systému z/OS je povoleno, je-li volba BFG_WTO nastavena na hodnotu YES, ON nebo TRUE. To řídí, zda se zprávy, které jsou zapsány do protokolu událostí agenta, zapisují také do zařízení protokolu operátora z/OS , což umožňuje snadnější přístup pro produkty automatizace, když spustíte agenta z JCL. Směrovací kód je Programmer Information (11) a deskriptorový kód je Informational (12).
SERVICE_TYPE-TYP služby	Určuje, zda je knihovna příkazů MFT určena pro agenta nebo modul protokolování. Platné hodnoty jsou AGENT nebo LOGGER.

Tabulka 44. Proměnné prostředí (pokračování)	
Proměnná prostředí	**Hodnota**
NÁZEV	Název agenta nebo modulu protokolování pro hodnotu SERVICE_TYPE.
QMGR	Název lokálního správce front, který je přidružen k agentovi nebo modulu protokolování pro hodnotu SERVICE_TYPE.
VÝSTUPNÍ_TŘÍDA	Výstupní třída pro datové sady SYSOUT. Výchozí hodnota *, která požaduje stejnou výstupní třídu jako parametr MSGCLASS z příkazu úlohy.
MQ_PATH	Cesta k adresáři komponent produktu IBM MQ for z/OS UNIX .
MQ_HLQ	Kvalifikátor vyšší úrovně pro datové sady IBM MQ .
MQ_LANG	Požadovaný jazyk.
DB2_HLQ	Volitelné. Kvalifikátor vyšší úrovně pro datové sady Db2 .
JOBCARD1	Řádek záhlaví 1 pro úlohu příkazu JCL.
JOBCARD2	Řádek záhlaví 2 pro úlohu příkazu JCL.
JOBCARD3	Řádek záhlaví 3 pro úlohu příkazu JCL.
ADMIN_JOB1	Řádek záhlaví 1 pro úlohu administrátora.
ADMIN_JOB2	Řádek záhlaví 2 pro administrativní úlohu.
ADMIN_JOB3	Řádek záhlaví 3 pro administrativní úlohu.
FTE_CONFIG	Existující konfigurace MFT pro migraci. Není-li migrace vyžadována, nastavte na prázdnou hodnotu.
CESTA_K_POVĚŘENÍ	Cesta k souboru pověření pro migraci, například `/u/user1/agent3`. Nezbytné pouze pro příkazy migrace **BFGAGMG** a skripty JCL **BFGLGMG** . Není-li migrace vyžadována, nastavte na prázdnou hodnotu. Všimněte si také, že
DB_PROPS_PATH	Určuje soubor vlastností modulu protokolování databáze pro migraci. Tato volba je vyžadována pouze v případě, že soubor vlastností nepoužívá následující výchozí název a cestu: `config_directory/coordination_qmgr/databaselogger.properties`. Není-li migrace vyžadována, nastavte na prázdnou hodnotu.

Následující tabulka popisuje povinné vlastnosti konfigurace MFT pro příkaz BFGSTDIN DD pro skript BFGCUSTM JCL v datové sadě knihovny PDSE příkazu MFT . Před odesláním úlohy BFGCUSTM musíte nahradit vlastnosti zadané substitučními hodnotami (tj. hodnoty uzavřené ve dvou znaménkách plus, + +) vhodnou neprázdnou hodnotou. Tyto vlastnosti definují přepisy pro vlastnosti konfigurace MFT . Můžete přidat vlastnosti agenta a modulu protokolování, chcete-li upravit agenty nebo moduly protokolování pro vaše prostředí. Seznam všech vlastností viz “Soubory vlastností konfigurace” na stránce 726.

Tabulka 45. Povinné vlastnosti konfigurace pro příkaz BFGSTDIN DD	
Vlastnost	**Hodnota**
coordinationQMgr	Název koordinačního správce front pro konfiguraci, ke které je agent nebo modul protokolování přidružen.
coordinationQMgrHostitel	Volitelné. Název hostitele systému, na kterém je spuštěn koordinační správce front. Ponecháte-li hodnotu této vlastnosti prázdnou, předpokládá se připojení v režimu vazeb.
coordinationQMgrPort	Volitelné. Číslo portu, na kterém koordinační správce front naslouchá. Tento parametr se používá pouze v případě, že pro vlastnost hostitele coordinationQMgrzadáte také neprázdnou hodnotu.
coordinationQMgrKanál	Volitelné. Kanál, který se má použít pro připojení ke koordinačnímu správci front. Tento parametr se používá pouze v případě, že pro vlastnost hostitele coordinationQMgrzadáte také neprázdnou hodnotu.
connectionQMgr	Název správce front příkazů pro konfiguraci, ke které je agent nebo modul protokolování přidružen.
connectionQMgrHostitel	Volitelné. Název hostitele systému, na kterém je spuštěn správce front příkazů. Ponecháte-li hodnotu této vlastnosti prázdnou, předpokládá se připojení v režimu vazeb.
Port connectionQMgr	Volitelné. Číslo portu, na kterém správce front příkazů naslouchá. Tento parametr se používá pouze v případě, že pro vlastnost hostitele connectionQMgrzadáte také neprázdnou hodnotu.
Kanál connectionQMgr	Volitelné. Kanál, který se má použít pro připojení ke správci front příkazů. Tento parametr se používá pouze v případě, že pro vlastnost hostitele connectionQMgrzadáte také neprázdnou hodnotu.

z/OS *Skripty JCL agenta a příkazu modulu protokolování z/OS*

Sada příkazů JCL, která je k dispozici v datové sadě knihovny PDSE příkazu MFT .

Tabulka 46. Příkazy JCL dostupné v datové sadě knihovny PDSE příkazu MFT	
Člen	**Popis nebo příkaz příkazového řádku fte**
BFGCOPY	Úloha pro vytvoření kopie této knihovny
BFGCUSTM	Úloha pro přizpůsobení této knihovny pro agenta nebo modul protokolování
BFGZCFCR	fteSetupKoordinace
BFGZCMCR	fteSetupPříkazy: vytvořte soubor MFT command.properties
BFGZAGCR	fteCreateAgent. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.

Tabulka 46. Příkazy JCL dostupné v datové sadě knihovny PDSE příkazu MFT (pokračování)	
Člen	**Popis nebo příkaz příkazového řádku fte**
BFGLGCRS	fteCreateLogger. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu LOGGER.
BFGZAGST	fteStartAgent. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGAGSTP	Procedura **fteStartAgent** . Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGZAGPI	ftePingAgent. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGZAGSP	fteStopAgent. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGZLGST	fteStartLogger. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu LOGGER.
BFGLGSTP	Procedura **fteStartLogger** . Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu LOGGER.
BFGZLGSP	fteStopLogger. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu LOGGER.
BFGZAGSH	fteShowAgentDetails. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGZLGSH	fteShowLoggerDetails. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu LOGGER.
BFGZCFDF	fteChangeDefaultConfiguration
BFGZAGCL	fteCleanAgent. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGZAGDE	fteDeleteAgent. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGZLGDE	fteDeleteModul protokolování. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu LOGGER.
BFGZPRSH	fteDisplayVerze
BFGZAGLI	fteListAgenti. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.

Tabulka 46. Příkazy JCL dostupné v datové sadě knihovny PDSE příkazu MFT (pokračování)	
Člen	**Popis nebo příkaz příkazového řádku fte**
BFGZMNLI	fteListMonitory
BFGZSTLI	fteListScheduledTransfers
BFGZTMLI	fteListŠablony
BFGXCROB	**fteObfuscate** ukázka
BFGZRAS	**fteRAS**
BFGZAGTC	fteSetAgentTracetrasování agenta. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu AGENT.
BFGZLGTC	fteSetLoggerTraceÚroveň. Vytvořeno pouze v případě, že nastavíte proměnnou SERVICE_TYPE na hodnotu LOGGER.
BFGXPRAN	**fteAnt** ukázka
BFGXTRCA	**fteCancelTransfer** ukázka
BFGXMNCR	**fteCreateMonitor** ukázka
BFGXTMCR	**fteCreateTemplate** ukázka
BFGXTRCR	**fteCreateTransfer** ukázka
BFGXMNDE	**fteDeleteMonitor** ukázka
BFGXSTDE	**fteDeleteScheduledTransfer** ukázka
BFGXTMDE	**fteDeleteTemplate** ukázka

Notes:

- JCL pro příkazy, které vytvářejí skripty MQSC nebo odstraňují odkazy, vás požádá o spuštění skriptu, ale tento skript již byl úlohou spuštěn.
- BFGZRAS vytvoří člena BFGRAS při spuštění úlohy BGCUSTM.

z/OS Provedení přenosu ověření

Jak provést převod, abyste zkontrolovali, že produkt pracuje správně.

Přejmenujte a upravte člena BFGTRCRS.

1. Přidejte `/*` před `%BFGCMD CMD=fteCreateTransfer -h`
2. Odeberte ostatní komentáře v členovi.
3. Zadejte název aktuálního agenta pro `-sa` a `-da`
4. Uložit JCL
5. Odeslat JCL

Tento soubor JCL se připojuje ke správci front příkazů.

z/OS Konfigurace úlohy protokolování

Úloha protokolování musí být spuštěna na stejném obrazu jako koordinační správce front. Můžete se přihlásit do souboru Db2.

Vytvoření úlohy protokolování

Zkopírujte PDSE, aby byl modul protokolování specifický pro PDSE. Například `user.MFT.LOGGER`.

Potřebujete-li použít jiný soubor pověření, vytvořte jej. Viz téma Konfigurace souboru MQMFTCredentials.xml na webu z/OS.

Přezkoumejte člena BFGCUSTM. Všimněte si, že velká část obsahu zůstává stejná z předchozího přizpůsobení.

Nicméně, musíte:

- Změna // SYSEXEC DD DSN=SCEN.FTE.JCL...
- Změňte LIBRARY tak, aby odpovídala PDSE agenta
- Změňte QMGR na název koordinačního správce front
- Nastavit parametr SERVICE_TYPE=LOGGER na hodnotu SERVICE_TYPE=
- Změňte NAME na název modulu protokolování (odpovídající PDSE)
- Přezkoumejte JOBCARD a změňte název úlohy tak, aby se název lišil od názvů úloh agentů.
- Přezkoumání BFG_JVM_PROPERTIES = "-Xmx1024M"

Pokud používáte modul protokolování Db2 , je užitečné vytvořit soubor, abyste mohli zachytit trasování systému Db2 , které vám pomůže identifikovat problémy Db2 .

Název souboru je uveden ve vlastnostech prostředí JVM, kde soubor vlastností trasování JDBC má obsah, jako např.

```
db2.jcc.traceDirectory=/u/johndoe/fte
db2.jcc.traceFile=jccTrace1
db2.jcc.traceFileAppend=false
# turn on all traces
# db2.jcc.traceLevel=-1
# turn off all traces
db2.jcc.traceLevel=0
```

Nastavit dvě vlastnosti prostředí JVM

```
BFG_JVM_PROPERTIES=-Ddb2.jcc.propertiesFile=/u/.../sql.properties
-Ddb2.jcc.ssid=DBCA
```

Kde `/u/.../sql.properties` je název vašeho souboru vlastností trasování Db2 a *DBCA* je název vašeho subsystému Db2 .

Odešlete tuto úlohu s tím, že úloha vyžaduje výlučný přístup k datové sadě. Všechny úlohy pro agenta mají názvy jako *BFGLG**.

Protokolování do souborů

Další informace o protokolování do adresáře Db2naleznete v části “Vytvoření úlohy protokolování při protokolování do souboru Db2” na stránce 723 .

Přejmenujte člena BFGLGCRS. Tato úloha aktualizuje soubory v adresáři Managed File Transfer (MFT) a používá CSQUTIL k vytvoření front specifických pro agenta v lokálním správci front.

Původní soubor má příkaz %BFGCMD `CMD=fteCreateLogger -h` , který vypisuje syntaxi příkazu.

Chcete-li vytvořit úlohu modulu protokolování, označte jako komentář %BFGCMD `CMD=fteCreateLogger -h` vložením `/*` před příkaz, ujistěte se, že sloupec jedna je prázdný.

Odeberte komentáře z druhého příkazu a nakonfigurujte příkazy. Příklad:

```
%BFGCMD CMD=fteCreateLogger   +
-p MQPH     +
-loggerQMgr MQPH      +
```

```
-loggerType FILE        +
-fileLoggerMode circular    +
-fileSize 5MB +
-fileCount 5 +
-p MQPH +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>'
LOGGER
```

Zkontrolujte výstup, abyste viděli, že byl úspěšně zpracován.

Tip: Zkopírujte název cesty souboru `logger.properties` z výstupu úlohy do členu v PDSE agenta.

Například kopírovat do členu APATH

```
/u/user_ID/fte/wmqmft/mqft/config/MQPH/loggers/LOGGER/logger.properties
```

To je užitečné, pokud potřebujete zobrazit soubor vlastností.

Přidejte adresář do tohoto souboru:

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/
```

Pokud protokolujete do souboru, soubory protokolu jsou uloženy v tomto adresáři, například `LOGGER0-20140522123654897.log`.

Trasovací soubory jsou v podadresáři protokolu, například

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/logs
```

Nyní můžete spustit úlohu protokolování.

Vytvoření úlohy protokolování při protokolování do souboru Db2

Přejmenujte člena BFGLGCRS.

Tato úloha aktualizuje soubory v adresáři MFT a používá CSQUTIL k vytvoření front specifických pro agenta v lokálním správci front.

Musíte vědět:

Tabulka 47. Db2 proměnné

Název Db2	**Příklad**
-dbName databaseName	Toto můžete získat z hodnoty umístění ve zprávě DSNL004I pro subsystém Db2 .
- dbDriver filePath	Například: `/db2/db2v10/jdbc/classes/db2jcc.jar`
-dbLib filePath	Například: `/db2/db2v10/jdbc/lib/libdb2jcct2zos_64.so`

Upravte soubor. Původní soubor má příkaz `%BFGCMD CMD=fteCreateLogger -h` , který vypisuje syntaxi příkazu.

Odeberte komentáře z druhého příkazu a nakonfigurujte příkazy. Například:

```
%BFGCMD CMD=fteCreateLogger   +
-p MQPH     +
-loggerQMgr MQPH      +
-loggerType DATABASE      +
-dbType DB2           +
-dbName DSNDBCP         +
-dbDriver /db2/db2v10/jdbc/classes/db2jcc.jar  +
-dbLib /db2/db2v10/jdbc/lib/            +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>' +
LOGGER
```

Chcete-li vytvořit úlohu modulu protokolování, označte jako komentář %BFGCMD CMD=fteCreateLogger -h vložením /* před příkaz, ujistěte se, že sloupec jedna je prázdný.

Odešlete úlohu a zkontrolujte výstup, abyste zjistili, že byla úspěšně zpracována.

Tip: Zkopírujte název cesty souboru `logger.properties` z výstupu úlohy do členu v PDSE agentů.

Například zkopírujte do členu APATH:

```
/u/user_ID/fte/wmqmft/mqft/config/MQPH/loggers/LOGGER/logger.properties into member USS
```

To je užitečné, pokud potřebujete zobrazit soubor vlastností

Trasovací soubory jsou v podadresáři protokolu, například:

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/logs
```

Vytvoření tabulek Db2

Musíte vytvořit tabulky Db2 . Definice jsou v souboru z/OS UNIX System Services `mqft/sql/ftelog_tables_zos.sql`.

Vytvořte člena Db2 ve svém PDSE. Upravte tento člen a použijte příkaz COPY na příkazovém řádku. Zkopírujte soubor definic z/OS UNIX System Services .

Vzhledem k tomu, že požadavky specifické pro org. jednotku se mohou značně lišit, tento soubor určuje pouze základní struktury tabulek a tabulkový prostor, kde budou umístěny.

Tabulkový prostor je určen skriptem SQL, aby se zajistilo, že je vytvořen pomocí fondu vyrovnávacích pamětí s velikostí stránky dostatečnou pro uložení největších možných řádků tabulek. Všimněte si, že nejsou zadány atributy, jako např. umístění objektů LOB atd.

Administrátor databáze může chtít upravit kopii tohoto souboru, aby definoval tyto atributy související s výkonem.

Tento soubor také předpokládá výchozí název schématu FTELOG, výchozí název tabulkového prostoru FTELOGTSa název databáze FTELOGDB. Tyto názvy můžete v případě potřeby změnit tak, aby odpovídaly existující databázi a jakýmkoli místním konvencím pojmenování, a to podle postupu popsaného v komentářích na začátku souboru.

Důležité: Ke spuštění příkazů použijte prostředky online, jako např. **SPUFI** , protože v souboru jsou komentáře a dávkové programy, jako je **DSNTINAD** , komentáře nepřijímají.

Další informace viz Provádění SQL pomocí SPUFI . Kromě toho má CSQ45STB v SCSQPROC ukázku JCL, kterou můžete upravit pro provedení příkazů Db2 SELECT.

Spuštění úlohy modulu protokolování

Přejmenujte, přezkoumejte a odešlete člena BFGLGST Měli byste získat zprávu BFGDB0023I: Modul protokolování dokončil aktivity spuštění a je nyní spuštěn.

Operace modulu protokolování

Chcete-li zobrazit stav modulu protokolování, přejmenujte, přezkoumejte a odešlete člena BFGLGSH

Chcete-li zastavit modul protokolování, přejmenujte jej, přezkoumejte a odešlete člena BFGLGSP.

z/OS Proměnné prostředí pro MFT on z/OS

Pokud spouštíte příkazy přímo z prostředí z/OS UNIX System Services (z/OS UNIX) nebo z vlastních skriptů JCL, musíte po přizpůsobení a konfiguraci nastavit řadu proměnných prostředí před spuštěním konfiguračních a administrativních skriptů poskytnutých produktem Managed File Transfer. Tyto proměnné musíte nastavit pro každého uživatele a v každém prostředí, ze kterého budou skripty vyvolány.

Chcete-li se vyhnout konfliktům s jinými produkty, můžete ve svém domovském adresáři vytvořit skript `.wmqfterc` . Skript `.wmqfterc` je poté vyvolán každým ze skriptů Managed File Transfer a můžete jej použít k poskytnutí vlastního nastavení prostředí pro Managed File Transfer.

Existuje také jedna volitelná proměnná prostředí, BFG_WTO, kterou můžete nastavit pro odesílání zpráv do protokolu operátora při spuštění agentů z JCL.

Tabulka 48. Požadované proměnné prostředí z/OS

Proměnná prostředí	**Hodnota**
BFG_JAVA_HOME	Umístění instalace produktu Java . Další informace o podporovaných úrovních produktu Java naleznete v tématu Systémové požadavky pro produkt IBM MQ.
BFG_DATA	Umístění datového adresáře pro Managed File Transfer for z/OS. Jedná se o cestu k souboru *DATA_DIR*.
STEPLIB	Musí zahrnovat následující datové sady IBM MQ : • SCSQAUTH • SCSQANLE • SCSQLOAD Chcete-li spustit komponentu modulu pro protokolování databáze v systému z/OS , musí modul STEPLIB obsahovat také následující datové sady Db2 v zobrazeném pořadí: • SDSNEXIT • SDSNLOD2 • SDSNLOAD

Následuje příklad `.profile` , který správně konfiguruje proměnné prostředí pro Managed File Transfer:

```
STEPLIB=MQM.V920.SCSQAUTH:MQM.V920.SCSQANLE:MQM.V920.SCSQLOAD
PATH=/u/fteuser/bin:/u/fteuser/J7.0/bin:/bin:/usr/bin:/u/fteuser/extras/bin:/bin:$PATH
BFG_JAVA_HOME=/u/fteuser/J7.0
BFG_DATA=/u/fteuser/DATA_DIR
export PATH STEPLIB BFG_JAVA_HOME BFG_DATA
```

Upozornění: Proměnná prostředí LIBPATH již není zapotřebí při volání příkazů **`fte*`** z prostředí z/OS UNIX a měla by být odebrána z existujícího skriptu `.wmqfterc` .

Volitelně můžete také nastavit následující proměnné prostředí:

Tabulka 49. Volitelná proměnná prostředí z/OS	
Proměnná prostředí	**Hodnota**
BFG_WTO	Jedna z následujících hodnot povolí BFG_WTO: • YES • ZAP • PRAVDA Jedna z následujících hodnot zakáže BFG_WTO. Tyto hodnoty nerozlišují malá a velká písmena. • NEDEFINOVÁNO • NO • VYP • NEPRAVDA Povoluje protokolování z/OS . Standardně je tato proměnná prostředí zakázána. Zprávy, které se zapisují do protokolu událostí agenta, se také zapisují do prostředku protokolu operátora z/OS , který umožňuje snadnější přístup pro produkty automatizace, když spustíte agenta z JCL. Směrovací kód je Programmer Information (11) a deskriptorový kód je Informational (12).
NÁZEV_SKUPINY_BFG_	Skupina souborů `mqm` je obvykle přidružena k souborům a příkazům konfiguračních dat Managed File Transfer . V důsledku toho mají všichni uživatelé, kteří jsou členy skupiny `mqm` , přístup a mohou provádět změny v konfiguraci produktu Managed File Transfer . Další informace viz Oprávnění systému souborů pro MFT v části IBM MQ. Pro systém z/OS je skupina souborů entitou systému souborů z/OS UNIX a skupina souborů `mqm` není nutně definována. Můžete definovat alternativní, existující skupinu systémů souborů z/OS UNIX pro soubory konfiguračních dat Managed File Transfer pomocí proměnné prostředí BFG_GROUP_NAME. Například na příkazovém řádku shellu z/OS UNIX : `export BFG_GROUP_NAME=FTEGB` který definuje skupinu FTEGB, která má být přidružena k libovolným následně vytvořeným konfiguračním souborům pro aktuální relaci z/OS UNIX . Parametr BFG_GROUP_NAME můžete nastavit na prázdnou hodnotu nebo jej můžete odebrat.

z/OS Soubory vlastností konfigurace

Souhrn vlastností, které se používají v produktu Managed File Transfer.

- Soubor MFT coordination.properties
- Soubor MFT command.properties
- Soubor MFT agent.properties
- Soubor vlastností konfigurace modulu protokolování

z/OS Konfigurace MFT pro správce ARM (z/OS Automatic Restart Manager)

Managed File Transfer je aplikace s povoleným ARM.

Než začnete

Další informace o povolení ARM a definování zásad ARM pro váš systém naleznete v tématu Použití z/OS správce automatického restartování (ARM).

Chcete-li použít schopnost modulu protokolování databáze MFT k automatickému restartování a opětovnému připojení k databázi Db2 , je ARM jediným podporovaným správcem restartování, který je k dispozici.

Informace o této úloze

Pomocí ARM lze agenty a moduly protokolování nakonfigurovat pro restart nastavením vlastností agenta/modulu protokolování armELEMTYPEa armELEMENT. Vlastnost armELEMTYPE definuje typ prvku ARM a vlastnost armELEMENT je název prvku, který má ARM registrovat:

- Můžete nastavit agenta ELEMTYPE na SYSBFGAG a armELEMENT lze nastavit tak, aby odpovídal názvu agenta.
- Můžete nastavit ELEMTYPE modulu protokolování na SYSBFGLG a armELEMENT lze nastavit tak, aby odpovídal názvu modulu protokolování.

Poznámka: Agenty a moduly protokolování, které jsou nakonfigurovány pro restart pomocí ARM, lze úspěšně spustit pouze z dávkové úlohy nebo ze spuštěné úlohy. Pokusy o přímé spuštění agenta nebo modulu protokolování z příkazového řádku z/OS UNIX System Services selžou s kódem příčiny chyby ARM.

Příklad

Následující příklad zásady restartování definuje agenta BFGFT7CAG1 jako závislého na správci front FT7C:

```
RESTART_ORDER
   LEVEL(3)
   ELEMENT_TYPE(SYSBFGAG,SYSBFGLG)

RESTART_GROUP(GROUP7C)
   ELEMENT(SYSMQMGRFT7C)
   ELEMENT(BFGFT7CAG1)
       RESTART_ATTEMPTS(3,300)
```

z/OS Příklad: Vytvoření JCL pro agenty Managed File Transfer v systému z/OS

Pomocí těchto informací vygenerujte některé JCL, které lze použít k vytvoření a spuštění agenta v systému IBM MQ for z/OS.

Kopírovat ukázkovou knihovnu

Proveďte následující postup:

1. Vytvořte kopii knihovny SCSQFCMD (viz “Kopírovat SCSQFCMD pro vytvoření knihovny JCL” na stránce 711) otevřením knihovny.

   Většina členů, kteří začínají na BFGX, BFGY nebo BFGZ, jsou šablony, které použijete k pozdějšímu vygenerování upraveného JCL pro agenta.

   Důležitým členem je BFGCOPY.
2. Otevřete BFGCOPY a nahraďte:

   + + dodané_knihovny + +
   s názvem knihovny SCSQFCMD, která byla instalována jako součást produktu.

   + + knihovna služeb + +
   s názvem knihovny, kterou chcete použít pro agenta (cílovou knihovnu).
3. Odešlete úlohu a máte novou knihovnu, kterou můžete použít.

Upravit BFGCUSTM

Proveďte následující postup:

1. Otevřete novou knihovnu, abyste mohli upravit člena BFGCUSTM (viz “Úprava člena BFGCUSTM” na stránce 711).
2. Upravte všechny parametry ve členu, které jsou uzavřeny do znaků ++ , a nahraďte je odpovídajícími hodnotami. Například změňte:

   + + mq_path + +
   Cesta k adresáři komponent z/OS UNIX System Services (z/OS UNIX). Například `/mqm/V9R2M0`.

   Poznámka: Existují tři instance této proměnné, které mají být nahrazeny.

   + + bfg_data + +
   Jedná se o adresář z/OS UNIX , ve kterém má být uložena konfigurace produktu IBM MQ Managed File Transfer for z/OS .

   + + typ_služby + +
   Ke slovu AGENT

   + + název_agenta + +
   Chcete-li být jménem svého agenta

Notes:

1. Některé položky, například `++options++` požadované pro parametr CLEAN_AGENT_PROPS, nejsou potřebné, a proto byste je měli odebrat.
2. Úplný seznam všech parametrů ve členu BFGCUSTM spolu s popisem hodnot, které by měly mít, naleznete v části “Než začnete konfigurovat MFT pro z/OS” na stránce 706 .

Odeslání JCL BFGCUSTM

Proveďte následující postup:

1. Odešlete úlohu.
2. Ukončete knihovnu v ISPF.

   To je nezbytné, protože úloha BFGCUSTM aktualizuje knihovnu a nemůže to udělat, když je knihovna otevřená.
3. Po dokončení úlohy se podívejte do protokolu úlohy.

   Zobrazí se řada zpráv, které označují, že v knihovně byli vytvořeni noví členové.

   Každý z těchto členů obsahuje kód JCL, který lze použít k provádění specifických úloh pro vašeho agenta. Seznam těchto členů spolu s příkazy IBM MQ Managed File Transfer , kterým odpovídají, naleznete v části “Skripty JCL agenta a příkazu modulu protokolování z/OS” na stránce 719 .

Odeslat BFGAGCR pro vytvoření agenta

Nový člen BFGAGCR obsahuje některé JCL, které vytváří agenta vyvoláním příkazu **fteCreateAgent** .

Proveďte následující postup:

1. Otevřete člena BFGAGCR.

   Měli byste vidět, že BFGAGCR byl naplněn názvem vašeho:

   - Agent
   - Správce front agenta
   - Koordinační správce front pro topologii MFT
2. Odeslat člena BFGAGCR.

   Když je člen spuštěn, je:

   - Vytvoří požadované konfigurační soubory pro vašeho agenta.
   - Připojí se ke správci front agenta a vytvoří systémové fronty, které agent potřebuje, pomocí CSQUTIL.
   - Zaregistruje agenta v koordinačním správci front.

Spusťte agenta odesláním BFGAGST

Proveďte následující postup:

1. Odešlete člena BFGAGST. Viz použití agenta , kde naleznete různé příkazy, které vám ukazují, že agent pracuje správně.
2. Po dokončení úlohy zkontrolujte, zda protokol úlohy obsahuje následující zprávy:

   ```
   BFGAG0058I: The agent has successfully initialized.
   BFGAG0059I: The agent has been successfully started.
   ```

   což znamená, že váš agent je spuštěn a připraven provádět spravované přenosy.

z/OS Přesun agenta MFT do nové oblasti LPAR systému z/OS

Někdy je nutné přesunout agenta IBM MQ Managed File Transfer for z/OS z jedné oblasti LPAR do jiné a zároveň zachovat agenta ve stejné topologii produktu IBM MQ Managed File Transfer se stejnou koordinací a správci front příkazů. Potřebné kroky závisí na tom, jak byl agent, který se migruje, původně vytvořen.

Informace o této úloze

Přesuňte agenta IBM MQ Managed File Transfer for z/OS jedním z následujících způsobů:

- Pokud byl agent původně vytvořen pomocí upravené verze knihovny SCSQFCMD, použijte knihovnu k jeho opětovnému vytvoření v nové oblasti LPAR.
- Pokud byl agent původně vytvořen spuštěním příkazů z/OS UNIX System Services (z/OS UNIX), použijte příkazy k jeho opětovnému vytvoření v nové oblasti LPAR.

Poznámka:

Naplánované přenosy a šablony přenosu jsou uloženy v koordinačním správci front pro topologii IBM MQ Managed File Transfer . Tato úloha předpokládá, že koordinační správce front není součástí práce přesunu. V tomto případě všechny naplánované přenosy a šablony přenosu přidružené k přesouvanému agentu zůstanou po dokončení přesunu v existujícím koordinačním správci front.

Procedura

- Přesuňte agenta vytvořeného pomocí upravené verze knihovny SCSQFCMD.

Pokud byl agent vytvořen pomocí upravené verze knihovny SCSQFCMD, můžete tuto knihovnu použít k opětovnému vytvoření prostředí IBM MQ Managed File Transfer for z/OS a konfiguraci agenta v nové logické oblasti. Postupujte takto:

1. Zkopírujte přizpůsobenou verzi knihovny z původní oblasti LPAR do nové oblasti LPAR.
2. Upravte člena BFGCUSTM v upravené verzi knihovny v nové oblasti LPAR a ujistěte se, že hodnoty parametrů jsou stále platné.
3. Spusťte člena BFGCUSTM v nové oblasti LPAR, abyste vytvořili všechny JCL potřebné ke konfiguraci prostředí a vytvoření agenta.
4. Spuštěním člena BFGCFCR definujte koordinačního správce front, který má agent používat v nové oblasti LPAR, a vytvořte adresářovou strukturu potřebnou k uložení konfigurace IBM MQ Managed File Transfer .
5. Dále spusťte člena BFGCMCR a definujte správce front příkazů, který má agent používat v nové oblasti LPAR.
6. Spusťte člena BFGAGCR, abyste znovu vytvořili agenta a jeho konfiguraci.
7. Ujistěte se, že systémové fronty používané agentem existují ve správci front pro tohoto agenta.

Pokud má přesouvaný agent přidružené monitory prostředků, musíte znovu vytvořit monitory na novém agentovi. Postupujte takto:

1. V původní oblasti LPAR spusťte člena BFGMNLI, abyste vyexportovali definice pro monitor prostředků přidružený k původnímu agentovi do souborů XML.
2. Zkopírujte soubory XML obsahující definice monitoru prostředků do nové oblasti LPAR.
3. Pomocí člena BFGMNCRS v knihovně SCSQFCMD v nové oblasti LPAR naimportujte definice monitoru prostředků uložené v souborech XML. To má za následek vytvoření monitorů na novém agentovi.

- Přesuňte agenta vytvořeného spuštěním příkazů v adresáři z/OS UNIX.

  Pokud byl agent původně vytvořen spuštěním příkazů z/OS UNIX , můžete použít příkazy k opětovnému vytvoření agenta na nové logické oblasti. Postupujte takto:

  1. Spuštěním příkazu fteSetupCoordination v nové oblasti LPAR definujte koordinačního správce front, který má agent používat, a vytvořte adresářovou strukturu potřebnou k uložení konfigurace produktu IBM MQ Managed File Transfer .
  2. Spusťte příkaz fteSetupCommands , abyste definovali správce front příkazů, který má agent používat v nové logické oblasti.
  3. Spusťte příkaz fteCreateAgent , abyste znovu vytvořili agenta a jeho konfiguraci.
  4. Ujistěte se, že systémové fronty používané agentem existují ve správci front pro tohoto agenta.

  Pokud má přesouvaný agent přidružené monitory prostředků, musíte znovu vytvořit monitory na novém agentovi. Postupujte takto:

  1. V původní oblasti LPAR spusťte příkaz fteListMonitors a zadejte parametr **-ox** , abyste vyexportovali definice monitoru prostředků přidružené k původnímu agentovi do souborů XML.
  2. Zkopírujte soubory XML obsahující definice monitoru prostředků do nové oblasti LPAR.
  3. Spusťte příkaz fteCreateMonitor v nové oblasti LPAR a zadejte parametr **-ix** , abyste naimportovali definice monitoru prostředků uložené v souborech XML. To má za následek vytvoření monitorů na novém agentovi.

V 9.3.0 z/OS Plánování infrastruktury MFT pomocí skupin sdílení front IBM MQ for z/OS

Pokud používáte produkt IBM MQ Managed File Transfer (MFT), je třeba zvážit následující situace, kdy je jeden nebo více agentů, příkazů nebo koordinačních správců front součástí skupiny sdílení front IBM MQ for z/OS .

Popis agentů, správců front příkazů a koordinačních správců front viz Přehled topologie MFT .

Správci front agenta

Agent MFT se obvykle připojuje k jednomu správci front agenta a používá lokální fronty, které jsou přístupné pouze pro tohoto správce front. Agent je informován o tom, ke kterému správci front se má připojit, a to zadáním názvu správce front při prvním vytvoření agenta.

Pomocí produktu IBM MQ for z/OSje možné vytvořit agenta a nahradit název správce front názvem skupiny sdílení front (QSG). To znamená, že agent se může připojit k libovolnému dostupnému správci front v rámci skupiny sdílení front, aby mohl provádět přenosy souborů. Pokud dojde k selhání správce front, ke kterému je agent aktuálně připojen, agent zjistí selhání a znovu se připojí k alternativnímu správci front v rámci skupiny sdílení front.

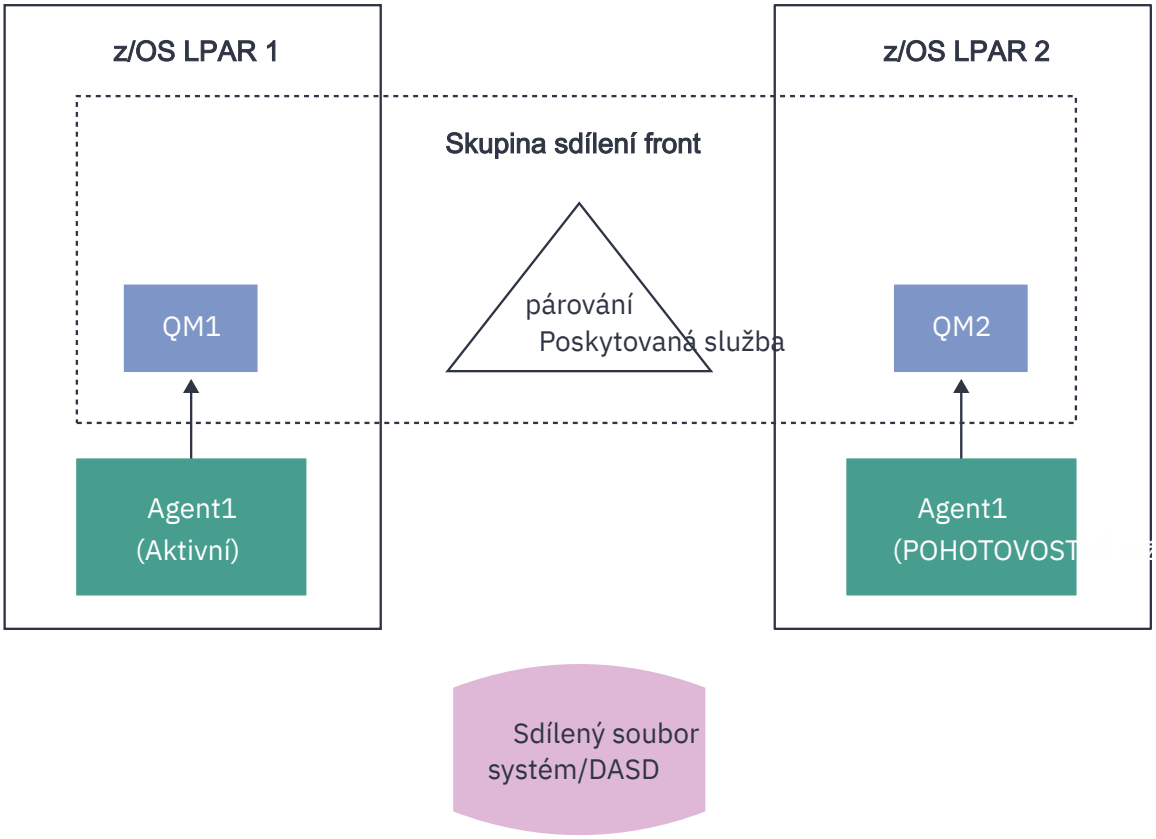
Připojení agenta k skupině sdílení front v kombinaci s podporou agenta s vysokou dostupností poskytovanou z produktu IBM MQ 9.2.0, viz téma “Vysoce dostupní agenti v produktu Managed File Transfer” na stránce 752, umožňuje vytvoření velmi robustních topologií MFT .

Například na následujícím obrázku *Agent1* byl vytvořen tak, že jeho správce front agenta je skupina správců front skládající se ze dvou správců front *QM1* a *QM2*. Fronty agenta byly definovány jako sdílené fronty uložené v prostředku Coupling Facility.

To znamená, že agent může být spuštěn na *LPAR 1* nebo *LPAR 2* a připojit se buď k *QM1* , nebo *QM2*. Soubory a datové sady, které agent čte z oblasti LPAR nebo do ní zapisuje, jsou sdílené, což znamená, že k nim lze přistupovat z oblasti LPAR.

Kromě toho byl agent nakonfigurován jako agent s vysokou dostupností. V diagramu je agent aktivní v *LPAR 1* a instance agenta v pohotovostním režimu je spuštěna v *LPAR 2*.

Tato topologie poskytuje vysokou odolnost. V případě selhání agenta spuštěného v oblasti *LPAR 1* nebo správce front *QM1* selhání, nebo *LPAR 1* selhání rezervní instance agenta v oblasti *LPAR 2* může převzít a pokračovat ve zpracování přenosů souborů od bodu selhání.



Obrázek 95. Agent MFT s vysokou dostupností používající skupinu sdílení front

Vytvoření agenta, který používá sdílení front jako správce front agenta

Agenta vytvoříte pomocí příkazu fteCreateAgent . Při této činnosti je pro správce front agenta poskytnut název skupiny sdílení front. Příklad:

```
fteCreateAgent -agentName Agent1 -agentQMgr QSG1
```

Tím se vytvoří agent s názvem *Agent1* , který jako správce front agenta používá libovolného správce front, který je členem skupiny QSG *QSG1* . V této konfiguraci se agent připojuje ke správci front agenta pomocí připojení s křížovou pamětí (režim vazeb), což znamená, že agent a správce front musí být ve stejné logické oblasti. To je přesně jako příklad znázorněný na obrázku 1 výše.

Když spustíte příkaz **fteCreateAgent** , vygeneruje sadu příkazů MQSC pro vytvoření nezbytných front ve správci front agenta.

Je-li správce front agenta QSG, je třeba tuto sadu příkazů upravit tak, aby byla každá fronta vytvořena jako sdílená fronta. To znamená, že každá fronta musí být vytvořena s QSGDISP (SHARED) a odpovídající strukturou prostředku Coupling Facility poskytovanou atributem CFSTRUCT.

Následující příklad ukazuje, jak změnit příkaz MQSC pro vytvoření SYSTEM.FTE.COMMAND.AGENT1 fronta jako sdílená fronta. Změny výchozích hodnot jsou uvedeny tučným písmem.

Důležité: Musíte provést podobné změny ve všech ostatních frontách, které agent používá.

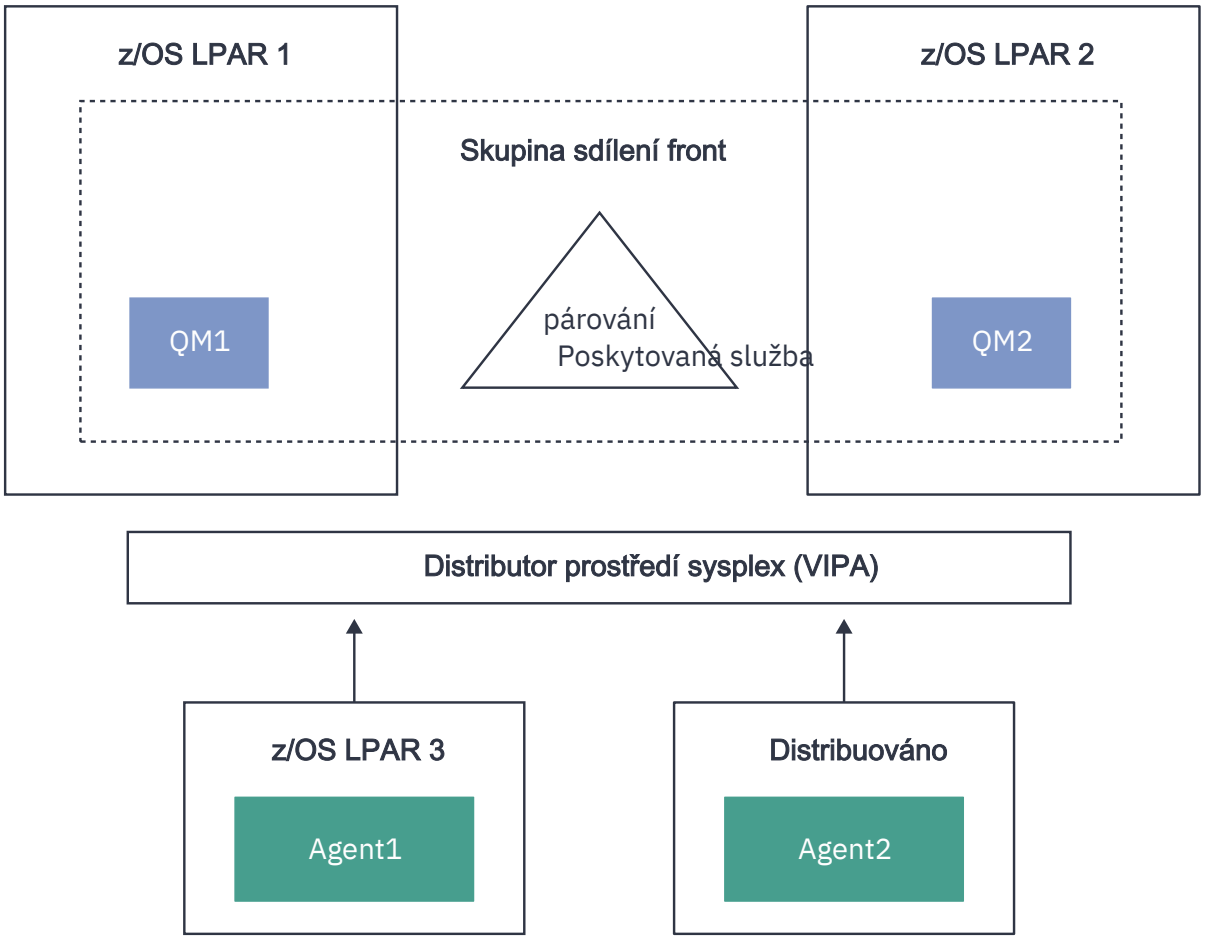
```
DEFINE QLOCAL(SYSTEM.FTE.COMMAND.AGENT1) +
 QSGDISP(SHARED) +
 CFSTRUCT(MFTSTRUCT) +
 DEFPRTY(0) +
 DEFSOPT(SHARED) +
 GET(ENABLED) +
 INDXTYPE(CORRELID) +
 MAXDEPTH(5000) +
 MAXMSGL(4194304) +
 MSGDLVSQ(PRIORITY) +
 PUT(ENABLED) +
 RETINTVL(999999999) +
 SHARE +
 NOTRIGGER +
 USAGE(NORMAL) +
 REPLACE
```

Vytvoření agenta, který používá skupiny sdílení front jako správce front agenta a připojuje se jako klient

Agenti se mohou připojit ke svému správci front agenta pomocí kanálu klienta. Tento přístup můžete použít k povolení spuštění agenta na distribuovaných platformách při připojení k QSG. Pokud jsou všichni správci front v rámci skupiny sdílení front licencováni pro produkt IBM MQ Advanced for z/OS Value Unit Edition, může se k nim agent také připojit z oblasti LPAR systému z/OS , která nemá lokálního správce front.

Tato topologie je zobrazena na následujícím obrázku a umožňuje agentovi využít schopnosti obnovy QSGs. Pokud dojde k selhání správce front v rámci skupiny sdílení front, ke kterému je agent aktuálně připojen, agent se automaticky znovu připojí k jinému členovi skupiny sdílení front a pokračuje ve zpracování.

Distributor prostředí sysplex se používá k rozložení připojení z agenta na dostupné správce front v rámci skupiny sdílení front.



Obrázek 96. Agenti MFT připojující se ke skupině sdílení front jako klient

Aby bylo možné používat tuto topologii, musí mít všichni správci front v rámci skupiny sdílení front definován kanál připojení serveru pro použití agentem. Informace o tom, jak to provést, naleznete v části “Připojení klienta ke skupině sdílení front” na stránce 61 .

Při vytváření agenta je třeba konfigurovat správce front, aby mohli používat kanál definovaný pro skupiny sdílení front a přistupovat k němu prostřednictvím distributora prostředí sysplex. Příklad:

```
fteCreateAgent -agentName Agent1 -agentQMgr QSG1 -agentQMgrHost vipaAddress
-agentQMgrPort sharedPort -agentQMgrChannel CHANNEL1
```

Jak již bylo uvedeno, příkazy MQSC generované spuštěním příkazu **fteCreateAgent** musí být upraveny tak, aby určovaly QSGDISP (SHARED) a odpovídající strukturu prostředku Coupling Facility v atributu CFSTRUCT.

Správci front příkazů

Správce front příkazů MFT může být součástí skupiny sdílení front. Název skupiny sdílení front však nelze použít při zadávání správce front příkazů. Musíte použít specifický název správce front.

Koordinační správci front

Koordinační správce front MFT může být součástí skupiny sdílení front. Stejně jako u správce front příkazů však nelze název skupiny sdílení front použít při zadávání koordinačního správce front. Musíte použít specifický název správce front.

Příkazy připojující se k QSG

Produkt MFT poskytuje řadu příkazů pro spravované agenty, přenosy a agenty, příkazy nebo koordinační správce front. Můžete použít pouze ty příkazy, které se připojují ke správci front agenta, pokud je správce front v QSG.

Následuje seznam příkazů, které se připojují ke správci front agenta:

- **fteCleanAgent**
- **fteCreateAgent**
- **fteCreateBridgeAgent**
- **fteCreateCDAgent**
- **fteDeleteAgent**

Při spouštění jiných příkazů MFT je třeba zadat název správce front.

Použití produktu Managed File Transfer for z/OS se spouštěcím programem JZOS Java

Pokyny v tomto tématu můžete použít jako alternativní metodu použití produktu Managed File Transfer ve vašem podniku na systému IBM MQ for z/OS .

Přehled

Managed File Transfer for z/OS (MFT) používá standardní instalační proceduru z/OS . Alternativním způsobem spuštění příkazů MFT je použití JCL a spouštěcího programu JZOS Java .

Další podrobnosti viz Spouštěcí program dávek JZOS a sada nástrojů .

Pokud se vašemu JCL nedaří správně zpracovat, prohlédněte si téma Společné problémy MFT s JZOS.

Příklad JCL

```
//JOHNDOEA JOB 1,MSGCLASS=H
// JCLLIB ORDER=(SCEN.MFT.JCL)   (1)
// INCLUDE MEMBER=BFGJCL8       (2)
//     DD * (2A)
. ${BFG_PROD}/bin/fteBatch createAgent  (3)
export IBM_JAVA_OPTIONS="${BFG_JAVA_OPTIONS} ${BFG_LANG}"  (4)
export JZOS_MAIN_ARGS="${BFG_MAIN_ARGS}" (4)
//MAINARGS DD *
-agentName MYAGENT  (5)
-f
-agentQMgr MQPD
-p MQPD
/*
```

kde:

- (1) Je umístění zahrnutých příkazů JCL
- (2) Zahrnout uvedeného člena JCL z umístění v 1)
- (2A) Toto rozšiřuje // STDENV-viz níže
- (3) Toto je příkaz, který se má provést, bez úvodní předpony fte
- (4) Tyto řádky jsou povinné, nastavují informace pro JZOS
- (5) Parametry příkazu
- Člen BFGJCL8 (můžete vybrat své vlastní jméno) vyvolá JZOS. Tento člen má STEPLIB a další JCL potřebné ke spuštění MFT.

Další JCL, které musíte zahrnout

Měli byste zahrnout JCL pro knihovny IBM MQ for z/OS , a pokud používáte modul protokolování Db2 , knihovny Db2 .

Příklad:

```
//WMQFTE EXEC PGM=JVMLDM86,REGION=0M PARM='+T'  (1)
//STEPLIB  DD DSN=SYS1.SIEALNKE,DISP=SHR        (2)
//* MQ libraries
//   DD DSN=MQM.V920.SCSQAUTH,DISP=SHR MQ Bindings
//   DD DSN=MQM.V920.SCSQANLE,DISP=SHR MQ Bindings
//   DD DSN=MQM.V920.SCSQLOAD,DISP=SHR MQ Bindings

//* DB2 libraries
//   DD DISP=SHR,DSN=SYS2.DB2.V12.SDSNEXIT.DBCP
//   DD DISP=SHR,DSN=SYS2.DB2.V12.SDSNLOAD
//   DD DISP=SHR,DSN=SYS2.DB2.V12.SDSNLOD2
//SYSOUT  DD SYSOUT=H
//SYSPRINT DD SYSOUT=H
//STDOUT  DD SYSOUT=H
//STDERR  DD SYSOUT=H

//STDENV  DD DSN=SCEN.MFT.JCL(BFGZENV8),DISP=SHR  (3)
```

kde:

- (1) Je název programu JZOS. Verzi ve vašem systému vyhledejte v adresáři SYS1.SIEALNKE . Přidat, PARM = '+ T' pro poskytnutí další diagnostiky.
- (2) Toto je datová sada s programem JZOS.
- (3) Toto je název člena skriptu shellu. Definuje parametry potřebné pro MFT. Viz téma “Skript shellu pro definování MFT” na stránce 735.

  Může to být libovolná datová sada a člen. Musí být poslední v souboru, protože úloha JCL toto rozšiřuje. Viz 2A v “Příklad JCL” na stránce 734.

Skript shellu pro definování MFT

V příkladu “Další JCL, které musíte zahrnout” na stránce 735 se použije člen BFGZENV8 . Toto je založeno na profilu JZOS.

Musíte vědět:

- Umístění, kde je nainstalován produkt Java
- Umístění knihoven IBM MQ for z/OS Java a MFT .
- ID uživatele musí být ve specifické skupině, aby bylo považováno za administrátora systému IBM MQ for z/OS . Potřebujete název této skupiny
- Pokud pro zprávy nepoužíváte angličtinu, musíte vědět, který jazyk zadat.

Ukázkový soubor

```
# This is a shell script that configures
# any environment variables for the Java JVM.
# Variables must be exported to be seen by the launcher.
# Use PARM='+T' and set -x to debug environment script problems
set -x
# . /etc/profile
#
# Java configuration (including MQ Java interface)
#
export _BPXK_AUTOCVT="ON"
export JAVA_HOME="/java/java71_bit64_sr3_fp30/J7.1_64/"
export PATH="/bin:${JAVA_HOME}/bin/classic/"
LIBPATH="/lib:/usr/lib:${JAVA_HOME}/bin"
LIBPATH="$LIBPATH:${JAVA_HOME}/bin/classic"
LIBPATH=$LIBPATH:"/mqm/V9R2M0/java/lib/"
export LIBPATH
```

```
export BFG_JAVA_HOME="${JAVA_HOME}"
export BFG_WTO="YES"
export BFG_GROUP_NAME=MQADM
export BFG_PROD="/mqm/V9R2M0/mqft"
export BFG_CONFIG="/u/johndoe/fteconfig"
# export BFG_LANG=" -Duser.language=de "
export BFG_LANG=" "

____________________
```

kde:

export _BPXK_AUTOCVT = "ON "
Je vyžadováno pro převod Unicode

export JAVA_HOME = "/java/java71_bit64/J7.1_64/"
Jedná se o umístění adresáře Java . Zadejte název cesty pro Java. Tento adresář obsahuje bin a další adresáře.

export PATH= "/bin: ${JAVA_HOME}/bin/classic/"
Nastaví příkaz cesty pro spustitelné příkazy Java

LIBPATH= "/lib:/usr/lib:${JAVA_HOME}/bin"
Nastaví cestu ke knihovně pro spustitelné příkazy Java

LIBPATH=" $LIBPATH: ${JAVA_HOME}/bin/classic"
Přidá další knihovny Java do příkazu LIBPATH.

LIBPATH=$LIBPATH: "/mqm/V9R2M0/java/lib/"
Přidá knihovny IBM MQ for z/OS do cesty ke knihovně. Zadejte název svých knihoven IBM MQ for z/OS v adresáři z/OS UNIX System Services.

export LIBPATH
Zpřístupní proměnnou LIBPATH pro systém JZOS

export BFG_JAVA_HOME = "${JAVA_HOME}"
Nastaví proměnnou BFG_JAVA_HOME na výše uvedenou hodnotu proměnné JAVA_HOME.

export BFG_WTO = "YES "
Nastavení BFG_WTO na hodnotu YES způsobí, že se zprávy zobrazí v protokolu úlohy pomocí WTO

export BFG_GROUP_NAME=MQADM
ID uživatelů, která jsou členem uvedené skupiny, jsou považována za administrátory produktu IBM MQ for z/OS .

export BFG_PROD = "/mqm/V9R2M0/mqft"
Je cesta, kde je umístěn kód MFT

export BFG_DATA= "/u/johndoe/fteconfig"
Je místo, kde jsou uloženy informace o konfiguraci MFT

 # export BFG_LANG = " -Duser.language= de"
Je komentovaný výrok definovat jazyk jako němčinu

export BFG_LANG = ""
Určuje jazyk jako výchozí angličtinu.

Obsah produktu MFT v adresáři `/lib/messages/BFGNVMessages_*.properties` uvádí seznam dostupných jazyků. Předvolba je ponechat hodnotu prázdnou, což znamená, že se použije angličtina.

Související úlohy

“Konfigurace produktu Managed File Transfer for z/OS” na stránce 705
Produkt Managed File Transfer for z/OS vyžaduje přizpůsobení, aby komponenta mohla správně fungovat.

Plánování pro Managed File Transfer

IBM i Konfigurace MFT na systému IBM i

Chcete-li začít používat produkt Managed File Transfer po jeho instalaci, musíte provést určitou konfiguraci koordinačního správce front a agenta.

Informace o této úloze

Po instalaci musíte spustit konfigurační skripty poskytované produktem Managed File Transfer pro nové koordinační správce front a nové agenty, než budete moci použít koordinační správce front a agenty k přenosu souborů. Poté musíte spustit agenty, které jste vytvořili.

Postup

1. Pro všechny nové koordinační správce front: spusťte příkazy MQSC v souboru *coordination_qmgr_name*.mqsc pro koordinačního správce front. Pokud se koordinační správce front nenachází ve stejném počítači jako instalace, zkopírujte skriptový soubor MQSC do počítače, ve kterém je umístěn správce front, a poté spusťte skript.
   a) Z příkazového řádku systému IBM i spusťte qshell pomocí následujícího příkazu: `CALL QSHELL`
   b) Přejděte do následujícího adresáře: `/QIBM/UserData/mqm/mqft/config/`*`coordination_qmgr_name`*
   c) Zadejte následující příkaz a nahraďte *coordination_qmgr_name* názvem svého správce front:

   ```
   /QSYS.LIB/QMQM.LIB/RUNMQSC.PGM coordination_qmgr_name < coordination_qmgr_name.mqsc
   ```

   Místo toho můžete koordinačního správce front nakonfigurovat ručně. Další informace viz téma "Konfigurace koordinačního správce front pro MFT" na stránce 741.
2. Pro všechny nové agenty: spusťte příkazy MQSC v souboru *agent_name*_create.mqsc pro správce front agenta.

   Pokud se správce front agenta nenachází ve stejném počítači jako agent, zkopírujte skriptový soubor MQSC do počítače, kde je správce front umístěn, a poté spusťte skript.
   a) Z příkazového řádku systému IBM i spusťte qshell pomocí následujícího příkazu: `CALL QSHELL`
   b) Přejděte do následujícího adresáře: `/QIBM/UserData/mqm/mqft/config/`*`agent_qmgr_name`*`/agents`
   c) Zadejte následující příkaz a nahraďte parametr *agent_qmgr_name* názvem správce front agenta a nahraďte parametr *název_agenta* názvem agenta:

   ```
   /QSYS.LIB/QMQM.LIB/RUNMQSC.PGM agent_qmgr_name < agent_name_create.mqsc
   ```

   Místo toho můžete nakonfigurovat správce front agenta ručně. Další informace viz "Konfigurace správců front agenta MFT" na stránce 747.
3. Pokud jste ještě nespustili subsystém QMFT jako součást instalace, spusťte z příkazového řádku IBM i subsystém QMFT pomocí následujícího příkazu: `STRSBS SBSD(QMQMMFT/QMFT)` nebo `STRSBS QMQMMFT/QMFT` .
4. Spusťte nové agenty pomocí příkazu **fteStartAgent** .
   a) Z příkazového řádku systému IBM i spusťte qshell pomocí následujícího příkazu: `CALL QSHELL`
   b) Přejděte do následujícího adresáře: `/QIBM/ProdData/mqm/bin`
   c) Zadejte následující příkaz a nahraďte AGENT názvem svého agenta:

   ```
   ./fteStartAgent AGENT
   ```

Jak pokračovat dále

Doporučuje se nastavit pískoviště pro omezení oblastí systému souborů, ke kterým má agent přístup. Tato funkce je popsána v části Práce s MFT pískovišti agenta.

Související pojmy

"Konfigurace produktu MFT pro první použití" na stránce 738
Některé konfigurační úlohy pro agenty Managed File Transfer a správce front musíte provést jednou, a to při prvním použití.

Konfigurace produktu MFT pro první použití

Některé konfigurační úlohy pro agenty Managed File Transfer a správce front musíte provést jednou, a to při prvním použití.

Související pojmy

“připojeníIBM MQ” na stránce 738
Veškerá síťová komunikace se správci front IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo jako kanály MQI.

“Konfigurace správce front pro více instancí pro práci s produktem MFT” na stránce 744
Produkt IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front pro více instancí se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agenta s více instancemi, koordinačnímu správci front s více instancemi a správci front příkazů s více instancemi.

Související úlohy

“Konfigurace síťových správců front MFT” na stránce 739
Pokud vaše síť Managed File Transfer obsahuje více než jednoho správce front IBM MQ , tito správci front IBM MQ musí být schopni vzájemně vzdáleně komunikovat.

“Konfigurace správců front agenta MFT” na stránce 747
Po instalaci spusťte skript *agent_name*_create.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name*/agents/*agent_name* a proveďte potřebnou konfiguraci pro správce front agenta. Chcete-li však tuto konfiguraci provést ručně, proveďte tyto kroky ve správci front agenta.

“Konfigurace koordinačního správce front pro MFT” na stránce 741
Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* , abyste provedli nezbytnou konfiguraci koordinačního správce front. Chcete-li však tuto konfiguraci provést ručně, proveďte v koordinačním správci front následující kroky.

“Vytvoření datové sady příkazu MFT Agent nebo Logger” na stránce 704
Datovou sadu PDSE příkazů můžete vytvořit z datové sady šablony příkazu Managed File Transfer pro specifickou Managed File Transfer Agent nebo Managed File Transfer Logger pro specifickou koordinaci.

“Aktualizace existující datové sady příkazu MFT Agent nebo Logger na systému z/OS” na stránce 715
Můžete aktualizovat datovou sadu knihovny PDSE příkazu Managed File Transfer , která je vytvořena z datové sady šablony příkazu Managed File Transfer .

Související odkazy

MFT Nastavení fronty agenta

MFT systémové fronty a téma systému

“Uchování zpráv protokolu MFT” na stránce 746
Produkt Managed File Transfer odesílá informace o průběhu přenosu souborů a protokolu do koordinačního správce front. Koordinační správce front publikuje tyto informace do všech odpovídajících odběrů v systému SYSTEM.FTE . Pokud nejsou k dispozici žádné odběry, nebudou tyto informace zachovány.

připojeníIBM MQ

Veškerá síťová komunikace se správci front IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo jako kanály MQI.

Managed File Transfer a kanály

Produkt Managed File Transfer používá kanály MQI k připojení agentů v režimu klienta ke svým správcům front agenta a k připojení příkazových aplikací (například **fteCreateTransfer**) ke svým příkazům a koordinačním správcům front. Ve výchozí konfiguraci jsou tato připojení vytvořena pomocí kanálu SVRCONN s názvem SYSTEM.DEF.SVRCONN, který standardně existuje ve všech správcích front.

Vzhledem k těmto výchozím nastavením nemusíte měnit žádné kanály MQI pro základní instalaci produktu Managed File Transfer .

Existuje šest typů koncových bodů kanálu zpráv, ale toto téma se týká pouze dvojic odesilatel-příjemce. Informace o dalších kombinacích kanálů naleznete v tématu Distribuované komponenty front .

Požadované cesty ke zprávám

Zprávy IBM MQ mohou cestovat pouze přes kanály zpráv, takže musíte zajistit, aby byly kanály k dispozici pro všechny cesty zpráv požadované produktem Managed File Transfer. Tyto cesty nemusí být přímé; zprávy mohou v případě potřeby procházet prostředními správci front. Toto téma se týká pouze přímé komunikace mezi dvěma body. Další informace o těchto volbách naleznete v tématu Jak se dostat ke vzdálenému správci front .

Komunikační cesty používané produktem Managed File Transfer jsou následující:

Agent pro agenta
: Všichni dva agenti, mezi kterými jsou soubory přenášeny, vyžadují obousměrnou komunikaci mezi přidruženými správci front. Vzhledem k tomu, že tato cesta nese hromadná data, zvažte možnost zkrácené, rychlé nebo levné cesty podle vašich potřeb.

Agent ke koordinaci
: Zprávy protokolu od agentů, kteří se účastní přenosu, musí být schopni dosáhnout koordinačního správce front.

Příkaz pro agenta
: Každý správce front, ke kterému se připojují příkazové aplikace nebo produkt IBM MQ Explorer (pomocí správce front příkazů), musí být schopen odesílat zprávy správcům front agentů, které tyto příkazové aplikace používají k řízení. Chcete-li povolit zobrazení zpráv zpětné vazby příkazy, použijte obousměrné připojení.

Další informace naleznete v tématu *Ověření IBM MQ* pro platformu nebo platformy, které používá váš podnik.

Související pojmy

“Konfigurace správce front pro více instancí pro práci s produktem MFT” na stránce 744
Produkt IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front pro více instancí se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agenta s více instancemi, koordinačnímu správci front s více instancemi a správci front příkazů s více instancemi.

Související úlohy

“Konfigurace síťových správců front MFT” na stránce 739
Pokud vaše síť Managed File Transfer obsahuje více než jednoho správce front IBM MQ , tito správci front IBM MQ musí být schopni vzájemně vzdáleně komunikovat.

“Konfigurace koordinačního správce front pro MFT” na stránce 741
Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* , abyste provedli nezbytnou konfiguraci koordinačního správce front. Chcete-li však tuto konfiguraci provést ručně, proveďte v koordinačním správci front následující kroky.

Konfigurace síťových správců front MFT

Pokud vaše síť Managed File Transfer obsahuje více než jednoho správce front IBM MQ , tito správci front IBM MQ musí být schopni vzájemně vzdáleně komunikovat.

Informace o této úloze

Existují dva způsoby, jak nakonfigurovat správce front tak, aby spolu mohli komunikovat:

- Nastavením klastru správce front IBM MQ .

Informace o klastrech správců front IBM MQ a jejich konfiguraci viz “Konfigurace klastru správců front” na stránce 284.

- Nastavením kanálů mezi správci front, které jsou popsány takto:

Nastavení kanálů mezi správci front

Nastavte následující kanály zpráv mezi správci front:

- Ze správce front agenta do koordinačního správce front
- Ze správce front příkazů do správce front agenta.
- Ze správce front agenta do správce front příkazů (chcete-li povolit zobrazování zpráv zpětné vazby příkazy).
- Ze správce front příkazů do koordinačního správce front
- Ze správce front agenta do libovolného jiného správce front agenta v síti Managed File Transfer .

Potřebujete-li další informace o způsobu nastavení této komunikace, začněte s těmito informacemi: Administrace vzdálených IBM MQ objektů pomocí MQSC.

Některé doporučené ukázkové kroky jsou:

Postup

1. Vytvořte přenosovou frontu ve správci front IBM MQ se stejným názvem jako koordinační správce front.
   Můžete použít následující příkaz MQSC:

   ```
   DEFINE QLOCAL(coordination-qmgr-name) USAGE(XMITQ)
   ```

2. Ve správci front IBM MQ vytvořte odesílací kanál pro koordinačního správce front Managed File Transfer .

   Název přenosové fronty vytvořené v předchozím kroku je povinný parametr pro tento kanál.

   Pro agenty v systému Managed File Transfer for IBM MQjsou zprávy publikovány s prázdným formátem.

   Můžete použít následující příkaz MQSC:

```
DEFINE CHANNEL(channel-name) CHLTYPE(SDR) CONNAME('coordination-qmgr-host(coordination-qmgr-port)')
 XMITQ(coordination-qmgr-name) CONVERT(NO)
```

   Poznámka: Nastavte hodnotu CONVERT (NO) pouze v případě potřeby.

3. V koordinačním správci front Managed File Transfer vytvořte přijímací kanál pro správce front IBM MQ . Přidělte tomuto přijímacímu kanálu stejný název jako odesílacímu kanálu ve správci front IBM MQ .
   Můžete použít následující příkaz MQSC:

   ```
   DEFINE CHANNEL(channel-name) CHLTYPE(RCVR)
   ```

Jak pokračovat dále

Dále postupujte podle kroků konfigurace koordinačního správce front: “Konfigurace koordinačního správce front pro MFT” na stránce 741.

Související pojmy

“připojeníIBM MQ” na stránce 738
Veškerá síťová komunikace se správci front IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo jako kanály MQI.

“Konfigurace správce front pro více instancí pro práci s produktem MFT” na stránce 744

Produkt IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front pro více instancí se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agenta s více instancemi, koordinačnímu správci front s více instancemi a správci front příkazů s více instancemi.

Související úlohy

“Konfigurace koordinačního správce front pro MFT” na stránce 741
Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* , abyste provedli nezbytnou konfiguraci koordinačního správce front. Chcete-li však tuto konfiguraci provést ručně, proveďte v koordinačním správci front následující kroky.

Konfigurace koordinačního správce front pro MFT

Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* , abyste provedli nezbytnou konfiguraci koordinačního správce front. Chcete-li však tuto konfiguraci provést ručně, proveďte v koordinačním správci front následující kroky.

Informace o této úloze

Postup

1. Vytvořte lokální frontu s názvem SYSTEM.FTE.
2. Přidejte SYSTEM.FTE do systému SYSTEM.QPUBSUB.QUEUE.NAMELIST .
3. Vytvořte téma s názvem SYSTEM.FTE s řetězcem tématu SYSTEM.FTE.
4. Ujistěte se, že atributy doručování dočasných zpráv (NPMSGDLV) a doručování trvalých zpráv (PMSGDLV) systému SYSTEM.FTE je nastaveno na hodnotu ALLAVAIL.
5. Zkontrolujte, zda je atribut PSMODE (režim publikování/odběru) koordinačního správce front nastaven na hodnotu ENABLED.

Jak pokračovat dále

Spustíte-li příkaz `strmqm -c` na správci front, který byl konfigurován jako koordinační správce front, příkaz odstraní změnu provedenou v kroku 2 (přidání SYSTEM.FTE do systému SYSTEM.QPUBSUB.QUEUE.NAMELIST seznam názvů). Důvodem je, že produkt `strmqm -c` znovu vytvoří výchozí objekty IBM MQ a vrátí změny Managed File Transfer . Proto, pokud jste spustili správce front s produktem `strmqm -c`, proveďte jeden z následujících kroků:

- Spusťte skript *coordination_qmgr_name*.mqsc ve správci front znovu.
- Opakujte krok 2.

Související pojmy

“připojeníIBM MQ” na stránce 738
Veškerá síťová komunikace se správci front IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo jako kanály MQI.

“Konfigurace správce front pro více instancí pro práci s produktem MFT” na stránce 744
Produkt IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front pro více instancí se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agenta s více instancemi, koordinačnímu správci front s více instancemi a správci front příkazů s více instancemi.

Související úlohy

“Konfigurace síťových správců front MFT” na stránce 739
Pokud vaše síť Managed File Transfer obsahuje více než jednoho správce front IBM MQ , tito správci front IBM MQ musí být schopni vzájemně vzdáleně komunikovat.

Související odkazy
fteSetupKoordinace

Vytvoření struktury přenosu souborů IBM MQ

Můžete konfigurovat strukturu Managed File Transfer na základě jednoho agenta připojeného ke správci front na stejném počítači.

Informace o této úloze

Konfigurace MFT je uložena ve struktuře souboru pod IBM MQ DataPathna počítači, na kterém bude agent umístěn.

Následující ukázková konfigurace je určena pro agenta MFT ve správci front IBM MQ 8.0 s názvem SAMPLECOORD (se zakázaným zabezpečením) a pro jednoho agenta MFT s názvem SAMPLEAGENT:

```
+--- config
             +--- SAMPLECOORD
                            +--- command.properties
                            +--- coordination.properties
                            +--- SAMPLECOORD.mqsc
                            +--- agents
                                           +--- SAMPLEAGENT
                                                          +--- agent.properties
                                                          +--- SAMPLEAGENT_create.mqsc
                                                          +--- SAMPLEAGENT_delete.mqsc

+---logs
             +--- SAMPLECOORD
                            +--- agents
                                           +--- SAMPLEAGENT
                                                          +--- logs
```

Tento příklad předpokládá, že zabezpečení správce front bylo zakázáno. Následující příkazy spuštěné v produktu **runmqsc**zakážou zabezpečení po restartování správce front:

```
runmqsc queue manager
 alter qmgr CONNAUTH(NONE);
 alter qmgr CHLAUTH(DISABLED);
 end;
```

Pro konfiguraci s povoleným zabezpečením v produktu MFT v produktu IBM MQ 8.0 nebo novějším produkt **CONNAUTH** vyžaduje, aby všechny příkazy MFT , které se připojují ke správci front, poskytovaly pověření pro ID uživatele a heslo. Pro každý příkaz můžete použít další parametry **-mquserid** a **-mqpassword** nebo můžete definovat soubor MQMFTCredentials.xml . Následující ukázkový soubor pověření definuje ID uživatele fteuser, pro který se má použít heslo produktu MyPassword při připojení ke správci front SAMPLECOORD:

```
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MQMFTCredentials"
        xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://wmqfte.ibm.com/MQMFTCredentials MQMFTCredentials.xsd">
    <tns:qmgr mqPassword="MyPassword" MyUserId="fteuser" name="SAMPELCOORD"/>
</tns:mqmftCredentials>
```

Další informace viz MFT a IBM MQ ověření připojení.

Notes:

- Chcete-li vyhledat konfigurační adresář MFT , použijte příkaz **fteDisplayVersion -v** .
- Pro uživatele systému z/OS může být soubor MQMFTCredential.xml umístěn jako člen v rozdělené datové sadě s formátem záznamu proměnné (RECFM = V) nebo nedefinovaným formátem záznamu (RECFM = U).
- V případě konfigurace s povoleným zabezpečením přidejte k níže uvedeným krokům následující parametr pro přidružení pověření k příslušnému správci front: -F *full_credential_file_path*.

- Heslo pro čistý text v souboru `MQMFTCredential.xml` lze zamlžené pomocí následujícího příkazu:

```
fteObfuscate -f full_file_path_to_MQMFTCredentials.xml
```

Postup

1. Vytvořte koordinačního správce front.

   Koordinační správce front je jediný správce front, který slouží k příjmu všech protokolů přenosu a informací o stavu od svých agentů. Spusťte následující příkaz:

   ```
   fteSetupCoordination -coordinationQMgr coordination_qmgr_name
   ```

   Tím se vytvoří základní konfigurace nejvyšší úrovně a vytvoří se IBM MQ skriptový soubor pro volání *coordination_qmgr_name*`.mqsc`.

   Konfiguraci je poté třeba načíst do správce front spuštěním následujícího příkazu IBM MQ :

   ```
   runmqsc queue manager name < coordination_qmgr_name.mqsc
   ```

   Poznámka: Pro připojení klienta TCP ke správci front můžete použít:

   ```
   fteSetupCoordination -coordinationQMgr coordination_qmgr_name
   -coordinationQMgrHost coordination_qmgr_host -coordinationQMgrPort coordination_qmgr_port
   -coordinationQMgrChannel coordination_qmgr_channel
   ```

   Pro vytvořený soubor *coordination_qmgr_name*`.mqsc`budete muset spustit příkaz **runmqsc** na stejném počítači, na kterém je spuštěn koordinační správce front.
2. Vytvořte správce front příkazů.

   Správce front příkazů je jediný správce front, který byl předkonfigurován tak, aby infrastruktura IBM MQ mohla směrovat požadavky MFT na příslušného agenta. Spusťte následující příkaz:

   ```
   fteSetupCommands -connectionQMgr Command QM Name -p Coordination QM Name
   ```

   Tím se vytvoří soubor `command.properties` v koordinačním adresáři. Všimněte si, že parametr `-p` je volitelný a není povinný, pokud jsou příkazy nastaveny pro výchozí koordinaci.

   Poznámka: Pro připojení klienta TCP ke správci front můžete použít:

   ```
   fteSetupCommands -p coordination_qmgr_name -commandQMgr connection_qmgr_name
   -commandQMgrHost connection_qmgr_host -commandQMgrPort connection_qmgr_port
   -commandQMgrChannel connection_qmgr_channel
   ```
3. Vytvořte agenta.

   Agent je aplikace, která může odesílat a přijímat soubory. Spusťte následující příkaz:

   ```
   fteCreateAgent -p coordination_qmgr_name -agentName agent_name -agentQMgr agent_qmgr_name
   ```

   Tím se vytvoří konfigurace agenta pod koordinací a vytvoří se skriptový soubor IBM MQ pro volání *agent_name*`.mqsc` v konfiguračním adresáři agenta.

   Spuštěním následujícího příkazu IBM MQ načtěte skriptový soubor IBM MQ do správce front:

   ```
   runmqsc agent_qmgr_name < agent_name_create.mqsc file
   ```

   Poznámka: Pro připojení klienta TCP ke správci front můžete použít:

   ```
   fteCreateAgent -p coordination_qmgr_name -agentName agent_name -agentQMgr agent_qmgr_name
   ```

```
-agentQMgrHost agent_qmgr_host -agentQMgrPort agent_qmgr_port -agentQMgrChannel
agent_qmgr_channel
```

4. Spusťte agenta.

   Spusťte následující příkaz:

   ```
   fteStartAgent -p coordination_qmgr_name agentName
   ```

   Agent se spustí na pozadí a vrátí se příkazový řádek. Chcete-li zkontrolovat, zda je agent spuštěn, spusťte tento příkaz:

   ```
   fteListAgents -p coordination_qmgr_name
   ```

   Zobrazuje stav agentů. Pokud je agent úspěšně spuštěn, je hlášen jako ve stavu READY.

Výsledky

Základní infrastruktura MFT je připravena k použití a nyní můžete použít příkaz **fteCreateTransfer** k vyžádání přenosu. Případně, je-li k dispozici IBM MQ Explorer , použijte k vytvoření a monitorování přenosů moduly plug-in MFT .

Další agenty lze přidat do konfigurace opakováním kroku 3: Vytvořte agenta. Pokud se používá připojení klienta TCP, mohou být na různých počítačích. Pro různé počítače musí být příkazy **fteSetupCoordination** a **fteSetupCommands** opakovány pro každý počítač, skripty mqsc však nemusí být spuštěny.

Složitější konfigurace mohou mít samostatné správce front pro koordinaci a každého agenta. V těchto případech bude nutné různé správce front spojit dohromady.

Související pojmy

Co dělat, když váš agent MFT není uveden v seznamu příkazem **fteListAgents**

Související odkazy

fteSetupKoordinace

Příkazy fteSetup: Vytvořte soubor MFT command.properties .

fteCreateAgent

fteObfuscate: šifrovat citlivá data

Formát souboru pověření MFT

Soubor MFT`agent.properties`

Konfigurace správce front pro více instancí pro práci s produktem MFT

Produkt IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front pro více instancí se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agenta s více instancemi, koordinačnímu správci front s více instancemi a správci front příkazů s více instancemi.

Konfigurace správce front pro více instancí

Důležité: Informace o konfiguraci IBM MQ správce front pro více instancí viz “Správci front s více instancemi” na stránce 493. Před pokusem o konfiguraci správce front s více instancemi pro práci s produktem Managed File Transferzkontrolujte, zda jste tyto informace četli.

Použití správce front s více instancemi jako správce front agenta

Chcete-li agentovi povolit připojení k aktivní i rezervní instanci správce front pro více instancí, přidejte vlastnost `agentQMgrStandby` do souboru `agent.properties` agenta. Vlastnost `agentQMgrStandby` definuje název hostitele a číslo portu použité pro připojení klienta pro instanci správce front

v pohotovostním režimu. Hodnota vlastnosti musí být zadána ve formátu MQ CONNAME, tj. *host_name*(*port_number*).

Vlastnost `agentQMgr` určuje název správce front pro více instancí. Vlastnost `agentQMgrHost` určuje název hostitele pro aktivní instanci správce front a vlastnost `agentQMgrPort` určuje číslo portu pro aktivní instanci správce front. Agent se musí připojit v režimu klienta k aktivní i rezervní instanci správce front s více instancemi.

Další informace viz Soubor MFT `agent.properties` .

Tento příklad zobrazuje obsah souboru `agent.properties` pro AGENT1 , který se připojuje ke správci front s více instancemi s názvem QM_JUPITER. Aktivní instance QM_JUPITER je na systému host1 a používá číslo portu 1414 pro připojení klienta. Pohotovostní instance QM_JUPITER je na systému host2 a používá číslo portu 1414 pro připojení klienta.

```
agentName=AGENT1
agentDesc=
agentQMgr=QM_JUPITER
agentQMgrPort=1414
agentQMgrHost=host1
agentQMgrChannel=SYSTEM.DEF.SVRCONN
agentQMgrStandby=host2(1414)
```

Použití správce front s více instancemi jako koordinačního správce front

Chcete-li povolit připojení k aktivní i rezervní instanci koordinačního správce front pro více instancí, přidejte vlastnost `coordinationQMgrStandby` do všech souborů `coordination.properties` ve vaší topologii Managed File Transfer .

Další informace viz Soubor MFT coordination.properties .

Tento příklad zobrazuje obsah souboru `coordination.properties` , který uvádí podrobnosti připojení ke správci front koordinace s více instancemi s názvem QM_SATURN. Aktivní instance QM_SATURN je v systému coordination_host1 a používá číslo portu 1420 pro připojení klienta. Rezervní instance QM_SATURN je v systému coordination_host2 a používá číslo portu 1420 pro připojení klienta.

```
coordinationQMgr=QM_SATURN
coordinationQMgrHost=coordination_host1
coordinationQMgrPort=1420
coordinationQMgrChannel=SYSTEM.DEF.SVRCONN
coordinationQMgrStandby=coordination_host2(1420)
```

Samostatný modul protokolování Managed File Transfer se musí vždy připojit ke svému správci front v režimu vazeb. Při použití samostatného modulu protokolování s koordinačním správcem front pro více instancí připojte samostatný modul protokolování v režimu vazeb k jinému správci front. Postup je popsán v části “Alternativní konfigurace pro samostatný modul protokolování MFT” na stránce 770. Musíte definovat kanály mezi samostatným správcem front modulu protokolování a koordinačním správcem front s názvem hostitele a číslem portu obou instancí koordinačního správce front pro více instancí. Informace o tom, jak to provést, viz “Správci front s více instancemi” na stránce 493.

Modul plug-in Managed File Transfer pro IBM MQ Explorer se připojuje ke koordinačnímu správci front v režimu klienta. Pokud dojde k selhání aktivní instance koordinačního správce front s více instancemi, bude záložní instance koordinačního správce front aktivní a modul plug-in se znovu připojí.

Příkazy Managed File Transfer **`fteList*`** a **`fteShowAgentDetails`** se připojují přímo ke koordinačnímu správci front. Pokud je aktivní instance koordinace s více instancemi nedostupná, tyto příkazy se pokusí připojit k rezervní instanci koordinačního správce front.

Použití správce front s více instancemi jako správce front příkazů

Chcete-li povolit připojení k aktivní i rezervní instanci správce front příkazů pro více instancí, přidejte vlastnost `connectionQMgrStandby` do všech souborů `command.properties` ve vaší topologii Managed File Transfer .

Další informace viz Soubor MFT command.properties .

V tomto příkladu je uveden obsah souboru `command.properties` , který určuje podrobnosti připojení ke správci front příkazů pro více instancí s názvem QM_MARS. Aktivní instance QM_MARS je na systému command_host1 a používá číslo portu 1424 pro připojení klienta. Záložní instance QM_MARS je na systému command_host2 a používá číslo portu 1424 pro připojení klienta.

```
connectionQMgr=QM_SATURN
connectionQMgrHost=command_host1
connectionQMgrPort=1424
connectionQMgrChannel=SYSTEM.DEF.SVRCONN
connectionQMgrStandby=command_host2(1424)
```

Související pojmy

“připojeníIBM MQ” na stránce 738
Veškerá síťová komunikace se správci front IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo jako kanály MQI.

Související úlohy

“Konfigurace síťových správců front MFT” na stránce 739
Pokud vaše síť Managed File Transfer obsahuje více než jednoho správce front IBM MQ , tito správci front IBM MQ musí být schopni vzájemně vzdáleně komunikovat.

“Konfigurace koordinačního správce front pro MFT” na stránce 741
Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* , abyste provedli nezbytnou konfiguraci koordinačního správce front. Chcete-li však tuto konfiguraci provést ručně, proveďte v koordinačním správci front následující kroky.

Uchování zpráv protokolu MFT

Produkt Managed File Transfer odesílá informace o průběhu přenosu souborů a protokolu do koordinačního správce front. Koordinační správce front publikuje tyto informace do všech odpovídajících odběrů v systému SYSTEM.FTE . Pokud nejsou k dispozici žádné odběry, nebudou tyto informace zachovány.

Způsoby, jak zajistit, aby byly informace uchovávány

Pokud jsou informace o průběhu přenosu nebo protokolu významné pro váš podnik, musíte provést jeden z následujících kroků, abyste se ujistili, že jsou informace uchovány:

- Modul pro protokolování databáze Managed File Transfer slouží ke kopírování zpráv publikovaných do systému SYSTEM.FTE/Log do databáze Oracle nebo Db2 .
- Definujte odběr pro SYSTEM.FTE , které ukládá publikování do fronty IBM MQ . Definujte tento odběr před přenosem přenosů souborů, abyste zajistili, že všechny zprávy o průběhu a zprávy protokolu budou ve frontě zachovány.
- Vytvořte aplikaci, která používá rozhraní fronty zpráv (MQI) nebo produkt IBM MQ JMS k vytvoření trvalého odběru, a zpracujte publikování, která jsou doručena k odběru. Tato aplikace musí být v provozu před přenosech souborů, aby se zajistilo, že aplikace obdrží všechny zprávy o průběhu a zprávy protokolu.

Každý z těchto přístupů je podrobněji popsán v následujících sekcích.

Při uchovávání informací protokolu nespoléhejte na modul plug-in IBM MQ Explorer .

Použití modulu protokolování databáze Managed File Transfer k uchování zpráv protokolu

Modul pro protokolování databáze je volitelnou komponentou produktu Managed File Transfer , kterou můžete použít ke kopírování informací o protokolu do databáze pro účely analýzy a auditování. Modul

pro protokolování databáze je samostatná aplikace Java , kterou instalujete na systém, který je hostitelem koordinačního správce front a databáze. Další informace o modulu protokolování databáze viz “Konfigurace modulu protokolování MFT” na stránce 757.

Uchování průběhu a zpráv protokolu pomocí modulu plug-in IBM MQ Explorer

Při prvním spuštění instance modulu plug-in IBM MQ Explorer vytvoří instance trvalý odběr v koordinačním správci front. Tento trvalý odběr se používá ke shromažďování informací, které jsou zobrazeny v zobrazeních **Protokol přenosu** a **Aktuální průběh přenosu** .

Název trvalého odběru má předponu, která ukazuje, že odběr byl vytvořen modulem plug-in IBM MQ Explorer MFT , názvem hostitele a jménem uživatele. Například `MQExplorer_MFT_Plugin_HOST_TJWatson`.

Tato předpona je přidána v případě, že administrátor chce odstranit trvalý odběr, který již není v aktivním použití instancí modulu plug-in IBM MQ Explorer .

Použití trvalého odběru v koordinačním správci front může způsobit sestavení zpráv v systému SYSTEM.MANAGED.DURABLE fronty. Máte-li síť s velkým objemem dat Managed File Transfer , používejte modul plug-in IBM MQ Explorer zřídka, nebo obojí, tato data zpráv mohou zaplnit lokální systém souborů.

Chcete-li zabránit této situaci, zadejte, aby modul plug-in IBM MQ Explorer používal pro koordinačního správce front netrvalý odběr. V produktu IBM MQ Explorer postupujte takto:

1. Vyberte položky **Okno** > **Předvolby** > **MQ Explorer** > **Managed File Transfer**
2. V seznamu **Typ odběru protokolu přenosu** vyberte NON_DURABLE.

Ukládání publikování ve frontě IBM MQ

Chcete-li ukládat zprávy protokolu nebo zprávy o průběhu ve frontě IBM MQ , konfigurujte odběr v koordinačním správci front, který předává zprávy do této fronty. Chcete-li například postoupit všechny zprávy protokolu do fronty s názvem LOG.QUEUE, odešlete následující příkaz MQSC:

```
define sub(MY.SUB) TOPICSTR('Log/#') TOPICOBJ(SYSTEM.FTE) DEST(LOG.QUEUE)WSCHEMA(TOPIC)
```

Poté, co byly zprávy protokolu postoupeny do fronty IBM MQ , jsou trvale uloženy ve frontě, dokud nejsou zpracovány aplikací IBM MQ , která tuto frontu používá.

Zápis aplikací, které spravují trvalý odběr, do systému SYSTEM.FTE

Do systému SYSTEM.FTE pomocí jednoho z rozhraní API podporovaných produktem IBM MQ. Tyto aplikace mohou přijímat zprávy fronty nebo protokolu produktu IBM MQ a pracovat s nimi odpovídajícím způsobem podle vašich obchodních potřeb.

Další informace o dostupných rozhraních API naleznete v tématu Vývoj aplikací.

Konfigurace správců front agenta MFT

Po instalaci spusťte skript *agent_name*`_create.mqsc` v adresáři *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/agents/`*agent_name* a proveďte potřebnou konfiguraci pro správce front agenta. Chcete-li však tuto konfiguraci provést ručně, proveďte tyto kroky ve správci front agenta.

Postup

1. Vytvořte fronty operací agenta.
   Tyto fronty jsou pojmenovány:
   - SYSTEM.FTE.COMMAND.*název_agenta*
   - SYSTEM.FTE.DATA.*název_agenta*
   - SYSTEM.FTE.EVENT.*název_agenta*

- SYSTEM.FTE.REPLY.*název_agenta*
- SYSTEM.FTE.STATE.*název_agenta*

Chcete-li získat informace o parametrech fronty a o tom, jak se fronty používají, prohlédněte MFT Nastavení fronty agenta.

2. Vytvořte fronty oprávnění agenta.

Tyto fronty jsou pojmenovány:

- SYSTEM.FTE.AUTHADM1.*název_agenta*
- SYSTEM.FTE.AUTHAGT1.*název_agenta*
- SYSTEM.FTE.AUTHMON1.*název_agenta*
- SYSTEM.FTE.AUTHOPS1.*název_agenta*
- SYSTEM.FTE.AUTHSCH1.*název_agenta*
- SYSTEM.FTE.AUTHTRN1.*název_agenta*

Chcete-li získat informace o parametrech fronty a o tom, jak se fronty používají, prohlédněte MFT Nastavení fronty agenta.

Jak pokračovat dále

Informace o vytvoření a konfiguraci agenta mostu protokolů viz fteCreateBridgeAgent (vytvoření a konfigurace MFT agenta mostu protokolů) a Konfigurace mostu protokolů pro server FTPS.

Související pojmy

“připojeníIBM MQ” na stránce 738
Veškerá síťová komunikace se správci front IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo jako kanály MQI.

“Konfigurace správce front pro více instancí pro práci s produktem MFT” na stránce 744
Produkt IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front pro více instancí se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agenta s více instancemi, koordinačnímu správci front s více instancemi a správci front příkazů s více instancemi.

Související úlohy

“Konfigurace síťových správců front MFT” na stránce 739
Pokud vaše síť Managed File Transfer obsahuje více než jednoho správce front IBM MQ , tito správci front IBM MQ musí být schopni vzájemně vzdáleně komunikovat.

“Konfigurace koordinačního správce front pro MFT” na stránce 741
Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* , abyste provedli nezbytnou konfiguraci koordinačního správce front. Chcete-li však tuto konfiguraci provést ručně, proveďte v koordinačním správci front následující kroky.

Související odkazy

MFT Nastavení fronty agenta

fteSetupKoordinace

Konfigurace agenta MFT pro více kanálů v klastru

Chcete-li v klastrované konfiguraci použít vícekanálovou podporu IBM MQ , nejprve nastavte vlastnost **agentMultipleChannelsEnabled** na hodnotu `true` a poté postupujte podle pokynů v tomto tématu.

Informace o této úloze

V klastru je podpora více kanálů povolena definicemi IBM MQ pouze ve správci front cílového agenta.

Kromě standardních kroků konfigurace IBM MQ požadovaných pro agenta Managed File Transfer , které jsou uvedeny v části “Konfigurace produktu MFT pro první použití” na stránce 738, musíte dokončit kroky v tomto tématu.

Následující příklady konfigurace používají příkazy **runmqsc** .

Postup

1. Definujte přijímací kanál klastru pro každý kanál, který chcete použít. Pokud například používáte dva kanály:

   ```
   DEFINE CHANNEL(TO.DESTQMGRNAME_1) CHLTYPE(CLUSRCVR) CLUSTER(MFTCLUSTER)
   DEFINE CHANNEL(TO.DESTQMGRNAME_2) CHLTYPE(CLUSRCVR) CLUSTER(MFTCLUSTER)
   ```

   kde:

   - *DESTQMGRNAME* je název správce front cílového agenta.
   - *MFTCLUSTER* je název klastru IBM MQ .

   Doporučuje se používat konvenci pojmenování *MFTCLUSTER*.*DESTMGRNAME*_n pro kanály, ale tato konvence není povinná.
2. Definujte alias správce front odpovídající jednotlivým kanálům. Příklad:

   ```
   DEFINE QREMOTE(SYSTEM.FTE.DESTQMGRNAME_1) RQMNAME(DESTQMGRNAME) CLUSTER(MFTCLUSTER)
   DEFINE QREMOTE(SYSTEM.FTE.DESTQMGRNAME_2) RQMNAME(DESTQMGRNAME) CLUSTER(MFTCLUSTER)
   ```

   Musíte použít SYSTEM.FTE.*DESTQMGRNAME_n* konvence pojmenování pro aliasy správce front , protože odesílající agent hledá aliasy správců front tohoto formátu. Čísla, která použijete pro *n* , musí začínat na 1 a musí být následná. Definice musí být v rámci celého klastru, aby byly k dispozici ve správci front zdrojového agenta.

   Aby zdrojový i cílový agent správně určili počet aliasů správce front, **nedefinujte** výchozí hodnotu XMITQ pro správce front.

Související úlohy

“Konfigurace agenta MFT pro více kanálů: neklastrovaný” na stránce 749
Chcete-li použít vícekanálovou podporu IBM MQ v neklastrované konfiguraci, nejprve nastavte vlastnost agentMultipleChannelsEnabled na hodnotu `true` a poté postupujte podle pokynů v tomto tématu.

Související odkazy

Soubor MFT `agent.properties`

Konfigurace agenta MFT pro více kanálů: neklastrovaný

Chcete-li použít vícekanálovou podporu IBM MQ v neklastrované konfiguraci, nejprve nastavte vlastnost agentMultipleChannelsEnabled na hodnotu `true` a poté postupujte podle pokynů v tomto tématu.

Informace o této úloze

V neklastrované konfiguraci je podpora více kanálů povolena definicemi IBM MQ ve správci front zdrojového i cílového agenta.

Kromě standardních kroků konfigurace IBM MQ požadovaných pro agenta Managed File Transfer , které jsou uvedeny v části “Konfigurace produktu MFT pro první použití” na stránce 738, musíte dokončit kroky v tomto tématu.

Následující kroky předpokládají, že pro komunikaci mezi zdrojovým a cílovým správcem front jsou používány kanály odesílatele.

Následující příklady konfigurace používají příkazy **runmqsc** .

Postup

1. Ve správci front cílového agenta definujte přijímací kanál pro každý kanál, který chcete použít. Pokud například používáte dva kanály:

   ```
   DEFINE CHANNEL(TO.DESTQMGRNAME_1) CHLTYPE(RCVR) TRPTYPE(TCP)
   DEFINE CHANNEL(TO.DESTQMGRNAME_2) CHLTYPE(RCVR) TRPTYPE(TCP)
   ```

   kde: DESTQMGRNAME je název správce front cílového agenta.

   Doporučuje se použít TO.DESTMGRNAME_n pro kanály, ale tato konvence není povinná. Názvy přijímacích kanálů se musí shodovat s odpovídajícími odesílacími kanály ve správci front zdrojového agenta.
2. Ve správci front zdrojového agenta definujte přenosovou frontu pro každý kanál, který chcete použít. Pokud například používáte dva kanály:

   ```
   DEFINE QLOCAL(DESTQMGRNAME_1) USAGE(XMITQ)
   DEFINE QLOCAL(DESTQMGRNAME_2) USAGE(XMITQ)
   ```

   Doporučuje se použít konvenci pojmenování DESTMGRNAME_n pro přenosové fronty, ale tato konvence není povinná. Na vámi definované přenosové fronty se odkazuje z definic kanálu odesilatele a z definic aliasů správce front v následujících krocích.
3. Ve správci front zdrojového agenta definujte odesílací kanál pro každý kanál, který chcete použít. Pokud například používáte dva kanály:

   ```
   DEFINE CHANNEL(TO.DESTQMGRNAME_1) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(DESTHOST:port)
   XMITQ(DESTQMGRNAME_1)
   DEFINE CHANNEL(TO.DESTQMGRNAME_2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(DESTHOST:port)
   XMITQ(DESTQMGRNAME_2)
   ```

   Doporučuje se použít TO.DESTMGRNAME_n konvence pojmenování pro kanály, ale tato konvence není povinná. Názvy odesílacích kanálů musí odpovídat odpovídajícím přijímacím kanálům ve správci front cílového agenta.
4. Ve správci front zdrojového agenta definujte alias správce front odpovídající jednotlivým kanálům. Příklad:

   ```
   DEFINE QREMOTE(SYSTEM.FTE.DESTQMGRNAME_1) RQMNAME(DESTQMGRNAME) XMITQ(DESTQMGRNAME_1)
   DEFINE QREMOTE(SYSTEM.FTE.DESTQMGRNAME_2) RQMNAME(DESTQMGRNAME) XMITQ(DESTQMGRNAME_2)
   ```

   Musíte použít SYSTEM.FTE.DESTQMGRNAME_n konvence pojmenování pro aliasy správce front, protože odesílající agent hledá aliasy správců front v tomto formátu. Čísla, která použijete pro *n* , musí začínat na 1 a musí být následná.

   Aby agent správně určil počet aliasů správce front, **nedefinujte** výchozí hodnotu XMITQ pro správce front.

Související úlohy

“Konfigurace agenta MFT pro více kanálů v klastru” na stránce 748
Chcete-li v klastrované konfiguraci použít vícekanálovou podporu IBM MQ , nejprve nastavte vlastnost **agentMultipleChannelsEnabled** na hodnotu `true` a poté postupujte podle pokynů v tomto tématu.

Související odkazy

Soubor MFT `agent.properties`

Windows Konfigurace agentů MFT pomocí MSCS

Nastavení agenta Managed File Transfer (MFT) Microsoft Cluster Service (MSCS) je podporováno, pokud je platforma podporována produktem MFT a je spuštěna jedna z verzí produktu Windows.

Informace o této úloze

Tato úloha popisuje dva scénáře, které můžete provést, abyste dosáhli překonání selhání agenta MFT :

- Scénář 1: Konfigurace agenta jako prostředku MSCS.
- Scénář 2: Konfigurace správce front agenta a agenta jako prostředků MSCS.

Procedura

Scénář 1: Konfigurace agenta jako prostředku MSCS

- Chcete-li nakonfigurovat agenta jako prostředek MSCS, postupujte takto:
  a) Nainstalujte produkt Managed File Transfer lokálně na každý počítač v klastru.

     Viz Instalace Managed File Transfer.

  b) Vytvořte agenta na primárním počítači v klastru.

     Agent by měl být konfigurován pro připojení ke správci front agenta pomocí přenosu CLIENT. Ujistěte se, že jste vytvořili všechny objekty ve správci front pro tohoto agenta. Chcete-li získat informace o tom, jak to provést, prohlédněte si téma Nastavení agenta.

  c) Upravte agenta tak, aby byl spuštěn jako služba systému Windows , a nakonfigurujte jej tak, aby se automaticky nespustil, když se produkt Windows restartuje nastavením pole **Typ spuštění** pro službu agenta v nástroji Windows Services na hodnotu `Manual`.

     Další informace naleznete v tématu Spuštění agenta MFT jako služby systému Windows.

  d) Zopakujte krok “2” na stránce 751 a krok “3” na stránce 751 scénáře 1 na sekundárním počítači.

     Tím je zajištěno, že struktura souborů pro protokoly, vlastnosti atd. existuje na jiném počítači v klastru. Všimněte si, že není třeba vytvářet objekty správce front jako v kroku “2” na stránce 751.

  e) Na primárním počítači přidejte agenta jako 'Generickou službu' pod řízení MSCS.

     Postupujte takto:

     a. Klepněte pravým tlačítkem myši na klastr a vyberte volbu **Role-> Přidat prostředek-> 'Generická služba'**.

     b. Ze seznamu služeb Windows vyberte službu agenta a dokončete průvodce konfigurací klepnutím na tlačítko **Další**.

     Služba agenta je nyní přidána jako prostředek MSCS. Pokud dojde k překonání selhání, služba agenta se spustí na druhém počítači.

Scénář 2: Konfigurace správce front agenta a agenta jako prostředků MSCS

- Chcete-li nakonfigurovat správce front agenta a agenta jako prostředky MSCS, postupujte takto:
  a) Konfigurujte správce front agenta tak, aby byl spuštěn jako prostředek MSCS.

     Informace o tom, jak to provést, viz “Vložení správce front pod řízení MSCS” na stránce 482.

  b) Vytvořte agenta na primárním počítači v klastru.

     Agent by měl být konfigurován pro připojení ke správci front agenta pomocí přenosu BINDINGS. Ujistěte se, že jste vytvořili všechny objekty ve správci front pro tohoto agenta. Chcete-li získat informace o tom, jak to provést, prohlédněte si téma Nastavení agenta.

  c) Upravte agenta tak, aby byl spuštěn jako služba systému Windows , a nakonfigurujte jej tak, aby se automaticky nespustil, když se produkt Windows restartuje nastavením pole **Typ spuštění** pro službu agenta v nástroji Windows Services na hodnotu `Manual`.

     Další informace naleznete v tématu Spuštění agenta MFT jako služby systému Windows.

  d) Ujistěte se, že správce front agenta (který je pod řízením MSCS) je spuštěn na sekundárním počítači.

     Agent vytvořený v tomto počítači se připojí ke správci front pomocí přenosu BINDINGS, a proto musí být při vytvoření agenta k dispozici.

  e) Zopakujte krok “2” na stránce 751 a krok “3” na stránce 751 scénáře 2 na sekundárním počítači.

     Tím je zajištěno, že struktura souborů pro protokoly, vlastnosti atd. existuje na jiném počítači v klastru. Všimněte si, že není třeba vytvářet objekty správce front jako v kroku “2” na stránce 751.

f) Přidejte agenta jako 'Generickou službu' pod řízením MSCS.

Postupujte takto:

a. Klepněte pravým tlačítkem myši na klastr a vyberte volbu **Role-> Přidat prostředek-> 'Generická služba'**.

b. Ze seznamu služeb Windows vyberte službu agenta a dokončete průvodce konfigurací klepnutím na tlačítko **Další**.

g) Upravte vlastnosti prostředku služby agenta a přidejte prostředek správce front do seznamu závislostí.

To zajistí, že prostředek správce front bude spuštěn před spuštěním agenta.

h) Přepněte prostředek správce front do režimu offline a poté přepněte prostředek agenta do režimu online. Ověřte, zda je spuštěn prostředek správce front i agent.

Dojde-li k překonání selhání, služba agenta a správce front agenta budou spuštěny na sekundárním počítači.

Vysoce dostupní agenti v produktu Managed File Transfer

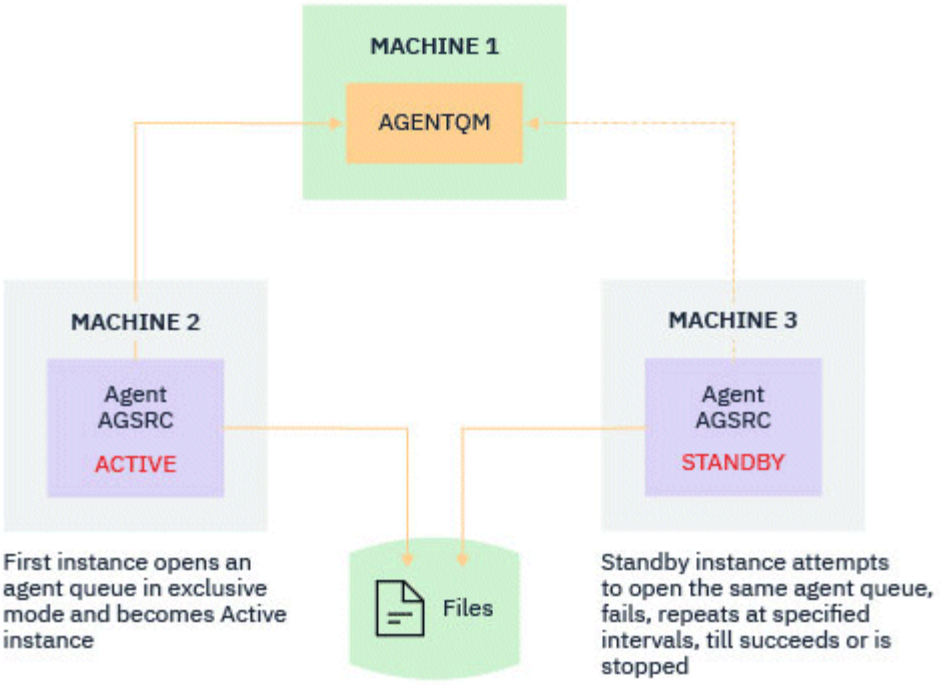
Můžete nakonfigurovat standardní agenty nebo agenty mostu v produktu MFT tak, aby se spouštěli v konfiguraci vysoké dostupnosti (HA). Dvojice instancí agenta s identickými konfiguracemi je zahrnuta v nastavení vysoké dostupnosti, kde jedna instance je spuštěna na jednom počítači, zatímco jiná instance je spuštěna na jiném počítači. Obě instance jsou konfigurovány pro připojení ke stejnému správci front agenta.

Přehled

Pouze jedna z těchto dvou instancí, nazývaných *aktivní instance*, zpracovává přenosy souborů, zatímco druhá instance, nazývaná *rezervní instance*, je v částečně inicializovaném stavu a nemůže zpracovat žádné přenosy souborů.

Pokud aktivní instance selže nebo ztratí konektivitu ke správci front, rezervní instance dokončí svou inicializaci, stane se aktivní a začne zpracovávat přenosy souborů. Všechny probíhající přenosy, které probíhaly v době, kdy se aktivní instance neúspěšně obnovila z posledního známého bodu kontroly.

Následující ilustrace ukazuje obecnou konfiguraci aktivních a rezervních



agentů:

Notes:

1. Jedna instance agenta je spuštěna na dvou různých počítačích, s jednou instancí jako *aktivní instance*a druhou jako *rezervní instance*.
2. Každá instance agenta je spuštěna na jiném počítači, s jednou z instancí jako aktivní instance a druhou jako rezervní instance.
3. Stejná sada front agenta je sdílena mezi oběma instancemi agenta.
4. Obě instance agenta potřebují přístup ke stejnému sdílenému systému souborů, aby mohly provádět spravované přenosy.

Mechanismus instance agenta aktivního pohotovostního režimu funguje tak, že se uzamkne na sdíleném prostředku. Instance agenta, která vezme zámek na sdíleném prostředku, se stane aktivní instancí, zatímco druhá instance (která se nepodaří zámek uzamknout) se stane rezervní instancí.

Sdílený prostředek je zde novou frontou, SYSTEM.FTE.HA.<agent name>. Tato fronta se vytvoří automaticky, když je konfigurován agent IBM MQ 9.1.4 nebo novější.

Jak proces funguje

Chcete-li vytvořit agenta HA, vytvořte agenta s identickými konfiguračními parametry na dvou počítačích spuštěním příkazu **fteCreateAgent** nebo **fteCreateBridgeAgent** pomocí dalšího parametru **-x** spolu s vlastností agenta **highlyAvailable** v souboru agent.properties nastaveném na hodnotu true.

Notes:

- Obě konfigurace musí ukazovat na stejného správce front agenta.
- Požadované fronty agenta musí být ve správci front agenta vytvořeny pouze jednou.

Další informace o vlastnosti agenta **highlyAvailable** viz příkaz **fteCreateAgent** , kde získáte další informace o parametru **-x** a souboru agent.properties .

Poznámka: Spuštěním příkazu **fteCreateAgent** nebo **fteCreateBridgeAgent** vytvoříte soubor MQSC obsahující skripty nezbytné pro vytvoření objektů IBM MQ ve správci front agenta a ve frontě SYSTEM.FTE.HA.*agent name* . Tento soubor MQSC je vytvořen bez ohledu na to, zda jste zadali parametr **-x** .

Při vytváření konfigurace agenta s vysokou dostupností příkaz **fteCreateAgent** nebo **fteCreateBridgeAgent** zkontroluje existenci instance stejného agenta přítomného na jiném místě přihlášením k odběru tématu SYSTEM.FTE/Agents/*agent name* . Pokud je nalezena instance stejného agenta, pak buď příkaz vytvoří požadovanou konfiguraci na systému souborů, ale nepublikuje vytvoření agenta znovu.

Když se agent spustí v režimu vysoké dostupnosti:

1. Agent se pokusí otevřít frontu SYSTEM.FTE.HA.*agent name* ve výlučném režimu GET.
2. Pokud agent úspěšně otevře frontu SYSTEM.FTE.HA.*agent name* , stane se *aktivní instancí* agenta a další proces spuštění bude pokračovat.
3. Pokud se pokus o otevření fronty SYSTEM.FTE.HA.*agent name* ve výlučném režimu GET nezdaří s kódem příčiny MQRC_OBJECT_IN_USE, znamená to, že již existuje aktivní instance agenta spuštěného jinde. Proto se tato instance stane *rezervní instancí* agenta.

   Rezervní instance se pokusí otevřít frontu SYSTEM.FTE.HA.*agent name* v uvedených intervalech. Pro tento účel je v souboru agent.properties poskytnuta další vlastnost agenta **standbyPollInterval** .

   S výchozí hodnotou se rezervní instance pokusí otevřít frontu SYSTEM.FTE.HA.*agent name* každých pět sekund. Toto se opakuje, dokud instance neúspěšně neotevře frontu SYSTEM.FTE.HA.*agent name* nebo dokud není zastavena pomocí příkazu **fteStopAgent** .

V produktu IBM MQ 9.2.4 a IBM MQ 9.2.0 Fix Pack 5je vlastnost **standbyPollInterval** také používána všemi instancemi k určení, jak dlouho instance čeká mezi pokusy o opětovné připojení, pokud je odpojena od svého správce front agenta.

Více instancí v pohotovostním režimu

Všechny rezervní instance se pokusí převzít frontu SYSTEM.FTE.HA.*agent name* ve výlučném režimu GET a instance, která je úspěšná po selhání aktivní instance, se stane aktivní instancí.

Aktivní instance udržuje informace o všech známých rezervních instancích a publikuje informace jako součást publikování stavu agenta. Výstup příkazu **fteShowAgentDetails** , odezva agenta GET REST API a modul plug-in IBM MQ Explorer MFT zobrazují informace o všech rezervních instancích.

Další informace viz příklad výstupů příkazu **fteShowAgentDetails** a odezvy agenta GET REST API .

Příklady informací o stavu agenta ve formátu XML viz MFT stavové zprávy agenta .

Požadavek na verzi

Aktivní a rezervní agenti musí být IBM MQ 9.1.4 nebo vyšší.

Upozornění:

- V režimech vysoké dostupnosti nelze konfigurovat ani spouštět verze produktu IBM MQ před verzí produktu IBM MQ 9.1.4 .
- Aktivní i rezervní instance musí spouštět stejnou verzi kódu.

Verze aktivních a rezervních instancí je ověřena, aby se zajistilo, že obě instance mají stejnou verzi. Dočasná dynamická fronta se používá pro komunikaci mezi instancemi. Dvě vlastnosti agenta, **dynamicQueuePrefix** a **modelQueueName**, definované v souboru agent.properties , generují název dočasné dynamické fronty.

Požadované informace pro agenty s vysokou dostupností v adresáři Managed File Transfer

Existují různé typy informací, které potřebujete vědět o standardních agentech nebo agentech mostu MFT , kteří jsou spuštěni v konfiguraci vysoké dostupnosti. Tyto informace zahrnují různé metody, kterými se agent spouští, jak identifikovat instanci agenta v souboru protokolu a informace o stavu agenta.

Spuštění agenta

Instance agenta je spuštěna v jiném režimu než v režimu vysoké dostupnosti

Pokud se pokusíte spustit jinou instanci agenta, který není konfigurován jako agent vysoké dostupnosti, nejprve se provede kontrola, zda lze zámek získat ve frontě SYSTEM.FTE.HA.*agent name* .

Vzhledem k tomu, že druhá instance byla spuštěna v jiném režimu než HA, zámek ve frontě SYSTEM.FTE.HA.*agent name* získá tato instance. Agent pokračuje v inicializaci, ale později selže, protože fronta příkazů je otevřena výhradně jinou instancí.

V tomto případě jsou zprávy zobrazené v následujícím příkladu protokolovány do souboru output0.log agenta a agent pokračuje ve svém pokusu o otevření fronty příkazů každých 30 sekund:

```
BFGMQ1045I: Systémová fronta agenta 'SYSTEM.FTE.COMMAND.SRC' je konfigurován buď jako NOSHARE,
nebo
Defsopt (sdíleno).

BFGAG0035W: Agent obdržel při pokusu o otevření fronty kód příčiny MQI 2042.
'SYSTEM.FTE.COMMAND.SRC've správci front' MFTHAQM 's názvem připojení' localhost (1414) '
a kanál 'MFT_HA_CHN'.  Agent se pokusí provést operaci znovu každých 30 sekund.
```

Instance agenta je spuštěna v režimu vysoké dostupnosti jinde

Pokud se pokusíte spustit jinou instanci agenta, který není konfigurován jako agent vysoké dostupnosti, nejprve se provede kontrola, zda lze zámek získat ve frontě SYSTEM.FTE.HA.*agent name* .

Vzhledem k tomu, že druhá instance byla spuštěna jako aktivní instance, pokus o získání zámku se nezdaří. Spuštění instance se nezdařilo a do souboru `output0.log` agenta se zaprotokoluje následující chybová zpráva:

```
BFGAG0194E: Instance tohoto agenta je již spuštěna jinde.
Proto tato instance nemůže pokračovat, a bude ukončena.
```

Windows Spuštění agenta jako Windows služba

V systému Windowsmůžete spustit agenta jako službu Windows .

Během spuštění produkt Windows spustí agenta MFT v normálním režimu nebo v režimu vysoké dostupnosti. Pokud je agent nakonfigurován pro spuštění v režimu vysoké dostupnosti, služba se spustí jako aktivní nebo rezervní instance, v závislosti na tom, která instance získá zámek jako první.

Identifikace typu instance agenta v souboru protokolu

Informační zprávy se zapisují do souboru `output0.log` agenta, aby označily typ instance. Když se instance agenta spustí jako aktivní instance, zapíše se tato zpráva:

```
BFGAG0193I: Agent byl úspěšně inicializován jako aktivní instance.
```

Když se instance agenta spustí jako instance v pohotovostním režimu, zapíše se tato zpráva:

```
BFGAG0193I: Agent byl úspěšně inicializován jako rezervní instance.
```

Aktualizace stavu agenta

Protože jsou spuštěny dvě instance stejného agenta, musíte mít informace o obou instancích v publikaci stavu agenta.

Všimněte si, že aktivní instance je ta, která publikuje stav obou instancí.

Rezervní instance

Při publikování stavu agenta aktivní instance kontroluje stáří publikování instance v pohotovostním režimu.

K tomuto účelu jsou v souboru `agent.properties` dvě další vlastnosti:

- **`standbyStatusExpiry`** je doba vypršení platnosti pro stavovou zprávu v pohotovostním režimu, která se má vložit do fronty příkazů agenta. Zpráva vyprší, pokud aktivní instance agenta nezpracuje tuto zprávu v tomto období.

  Standardně je hodnota **`standbyStatusExipry`** 30 sekund. Zpráva má také nízkou prioritu, 9, zprávu umožňující zpracování priority požadavků na přenos přes stavové zprávy v pohotovostním režimu.
- **`standbyStatusPublishInterval`** nastavuje frekvenci, se kterou rezervní instance publikuje svůj stav.

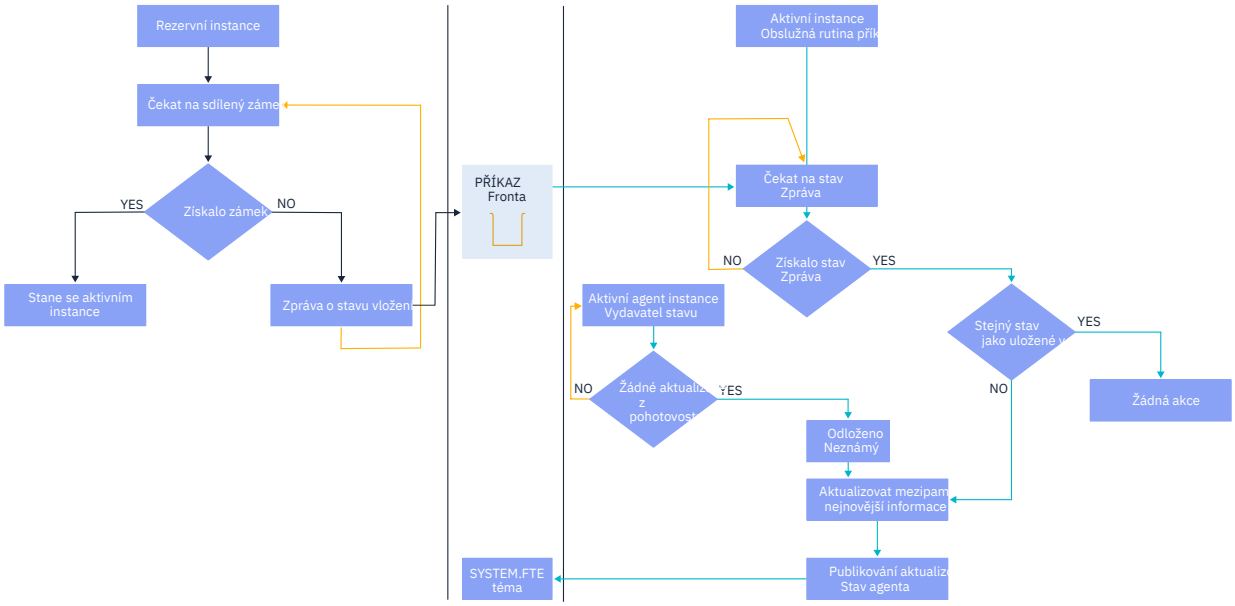
Aktivní instance

Aktivní instance provádí následující zpracování aktualizací stavu z rezervní instance:

1. Získá zprávu z fronty `SYSTEM.FTE.COMMAND.<agent name>` a deleguje zpracování zprávy na pracovní podproces.
2. Pracovní podproces načte obsah z těla zprávy, aktualizuje objekt stavu agenta pomocí informací o instanci v pohotovostním režimu a upozorní vydavatele stavu agenta, aby publikoval stav.
3. Vydavatel stavu agenta publikuje stav.

   Všimněte si, že zde jsou provedeny optimalizace pro uložení informací o stavu rezervní databáze do mezipaměti. Když je vydán požadavek, vydavatel stavu agenta zkontroluje nový stav se stavem uloženým v mezipaměti a publikuje pouze v případě, že existuje rozdíl.

Následující diagram popisuje tok, který následují aktivní nebo rezervní instance pro publikování stavu agenta:



Vyřazení instancí, překonání selhání a údržba ve vysoce dostupných agentech

Vysoce dostupné instance produktu Managed File Transfer mohou být vyřazeny, mohou selhat různými způsoby a mohou vyžadovat údržbu.

Vyřazení stavu rezervní instance

Mohou se vyskytovat situace, kdy je aktivní instance zaneprázdněna přenosy a nemůže zpracovat stavové zprávy instance v pohotovostním režimu, nebo instance v pohotovostním režimu selhala, nebo z jakéhokoli důvodu nepublikuje stavové zprávy.

V takových scénářích aktivní agent, který si byl vědom přítomnosti rezervní instance, čeká na hodnotu určenou vlastností **standbyStatusDiscardTime** v souboru `agent.properties` před odebráním rezervní instance z jejího seznamu. Výchozí hodnota této vlastnosti je 600 sekund, což je dvojnásobek hodnoty vlastnosti **standbyStatusPublishInterval** .

Selhání přes instanci normálně

Chcete-li provést normální překonání selhání, musíte použít příkaz **fteStopAgent** s volbou **-i** .

To zajistí, že aktivní instance bude okamžitě zastavena. Pokud zastavíte agenta bez volby **-i** , agent bude pokračovat v činnosti, dokud aktivní instance nedokončí všechny probíhající přenosy, takže překonání selhání může trvat dlouho.

Veškeré přenosy v inflight pokračují od posledního známého bodu kontroly.

Selhání nad instancí v jiných situacích

Pokud aktivní instance skončí způsobem, který není normální, nebo pokud dojde k selhání celého počítače, připojení k frontě agenta bude přerušeno a správce front zavře všechny otevřené fronty včetně fronty SYSTEM.FTE.HA.<agent name> a připojení.

Kvůli tomu rezervní instance získá výlučný příkaz GET a dokončí zbytek inicializace agenta.

Opět platí, že veškeré přenosy z inflight pokračují z posledních známých bodů kontroly.

Pokud dojde k přerušení připojení ke správci front.

Režim klienta

Proces agenta se skládá z několika podprocesů. Kromě výchozích podprocesů, například podprocesu, který publikuje stav agenta v pravidelných intervalech, je každý požadavek na přenos zpracován sadou podprocesů, které skončí po dokončení přenosu.

Mnoho z těchto podprocesů se připojí ke správci front agenta a vloží a získá zprávy. Je možné, že některá z těchto připojení mohou být přerušena kvůli problému se sítí nebo selhání správce front. Pokud některý podproces zjistí problém s přerušením připojení, informuje hlavní podproces o zahájení obnovy a ukončí se.

Hlavní podproces poté spustí další podproces, který bude čekat na připojení k navázané správci front. Po opětovném připojení dojde k pokusu o získání výlučného příkazu GET pro agenta. Pokud se to podaří, agent pokračuje v dokončování obnovy a stane se aktivní instancí. Pokud se pokus o získání výlučného příkazu GET nezdaří, instance se stane rezervní databází.

Režim vazeb

Pokud při připojování v režimu vazeb agent ztratí připojení, proces agenta skončí. Řadič procesů zpracovává restartování agenta. Když se agent restartuje, prochází procesem pokusu o získání výlučného GET pro sebe.

Pokud je agent úspěšný, stane se aktivní instancí; jinak se agent stane rezervní instancí.

Použití upgradů úrovně údržby

Kroky pro použití údržby na agenty s vysokou dostupností jsou podobné těm, které jsou dokumentovány pro správce front s více instancemi. Další informace naleznete v tématu Použití aktualizací úrovně údržby pro správce front s více instancemi v systému Windows nebo Použití aktualizací úrovně údržby pro správce front s více instancemi v systému AIXnebo Použití aktualizací úrovně údržby pro správce front s více instancemi v systému Linux.

Před použitím údržby musíte zastavit agenta spuštěného na počítači, na kterém se má použít úroveň údržby. Pokud aktualizujete aktivní instanci, musíte pro zajištění kontinuity přenosů provést překonání selhání aktivní instance na záložní instanci.

Po dokončení upgradu musíte spustit instanci agenta, převést aktuální aktivní instanci na upgradovanou instanci a poté upgradovat instanci v pohotovostním režimu.

Migrace agentů z dřívější verze produktu

Agenti migrovaní z verzí produktu IBM MQ před IBM MQ 9.1.4 jsou spuštěni jako nevysoce dostupní. Můžete je spustit v režimu vysoké dostupnosti podle postupu v části Migrace Managed File Transfer agentů z dřívější verze.

Konfigurace modulu protokolování MFT

Když produkt Managed File Transfer přenáší soubory, publikuje informace o svých akcích do tématu v koordinačním správci front. Modul pro protokolování databáze je volitelnou komponentou produktu Managed File Transfer , kterou můžete použít ke zkopírování těchto informací do databáze pro účely analýzy a auditování.

Existují tři verze modulu protokolování:

- ALW samostatný modul protokolování souborů
- samostatný modul pro protokolování databáze
- Modul protokolování Java Platform, Enterprise Edition (Java EE)

Moduly protokolování na systému IBM i

IBM i

Moduly protokolování Managed File Transfer nejsou na platformě IBM i podporovány.

Samostatný modul protokolování souborů

ALW

Samostatný modul protokolování souborů je proces Java , který je spuštěn v systému, který je hostitelem koordinačního správce front, nebo v systému, který je hostitelem správce front s konektivitou ke koordinačnímu správci front. Samostatný modul protokolování souborů používá vazby IBM MQ pro připojení k přidruženému správci front. Samostatný modul protokolování je vytvořen pomocí příkazu **fteCreateLogger** .

Windows Samostatný modul protokolování souborů můžete spustit jako službu systému Windows , abyste se ujistili, že modul protokolování souborů bude pokračovat v běhu, když se odhlásíte z relace Windows , a lze jej nakonfigurovat tak, aby se automaticky spustil, když se systém restartuje. Další informace viz téma “Instalace samostatného modulu protokolování souborů MFT” na stránce 759.

Samostatný modul protokolování souborů není podporován na následujících platformách:

- z/OS z/OS
- IBM i IBM i

Samostatný modul pro protokolování databáze

Samostatný modul pro protokolování databáze je aplikace Java , kterou instalujete v systému, který je hostitelem správce front a databáze. Samostatný modul pro protokolování databáze je často instalován ve stejném systému jako koordinační správce front, může však být instalován ve stejném systému jako kterýkoli správce front, který má konektivitu ke koordinačnímu správci front. Modul pro protokolování samostatné databáze používá vazby IBM MQ pro připojení k přidruženému správci front a ovladač JDBC typu 2 nebo 4 pro připojení k databázi Db2 nebo Oracle . Tyto typy připojení jsou nezbytné, protože samostatný modul pro protokolování databáze používá podporu XA správce front ke koordinaci globální transakce v rámci správce front i databáze a k ochraně dat.

Windows Používáte-li systém Windows , můžete spustit samostatné zapisovače protokolu jako služby systému Windows , abyste se ujistili, že zapisovače protokolu budou i nadále spuštěny, když se odhlásíte z relace Windows . Další informace naleznete v tématu “Instalace samostatného modulu protokolování databáze MFT” na stránce 766 pro samostatný modul pro protokolování databáze.

Modul pro protokolování databáze Java EE

Modul pro protokolování databáze Java EE je poskytován jako soubor EAR, který instalujete na aplikační server. To může být pohodlnější než použití samostatného modulu pro protokolování databáze, máte-li k dispozici existující prostředí aplikačního serveru Java EE , protože modul pro protokolování databáze Java EE lze spravovat společně s ostatními podnikovými aplikacemi. Modul pro protokolování databáze Java EE můžete také nainstalovat na samostatný systém do systémů, které jsou hostitelem serveru a databáze IBM MQ . Modul pro protokolování databáze Java EE je podporován pro použití s databázemi Db2 a Oracle . Modul pro protokolování databáze Java EE také podporuje produkt Oracle Real Application Clusters, je-li nainstalován na systému WebSphere Application Server 7.0.

Pokyny, jak konfigurovat modul protokolování, naleznete v následujících tématech:

- “Instalace samostatného modulu protokolování souborů MFT” na stránce 759
- “Instalace samostatného modulu protokolování databáze MFT” na stránce 766
- “Instalace modulu protokolování databáze Java EE pro MFT” na stránce 771

Související úlohy

“Použití MFT se vzdálenou databází” na stránce 768
Modul protokolování Managed File Transfer můžete použít ke komunikaci s databází na vzdáleném systému.

Související odkazy

Ošetření chyb a odmítnutí zprávy modulu protokolování MFT

Vlastnosti konfigurace modulu protokolování MFT

ALW Instalace samostatného modulu protokolování souborů MFT

Samostatný modul protokolování souborů je proces Java , který se musí připojit ke koordinačnímu správci front pomocí režimu vazeb IBM MQ nebo režimu klienta. Chcete-li definovat samostatný modul protokolování souborů, použijte příkaz **fteCreateLogger** a postupujte podle kroků v tomto tématu.

Informace o této úloze

Další informace o samostatném modulu protokolování souborů viz “Konfigurace modulu protokolování MFT” na stránce 757. Kroky v tomto tématu konfigurují modul protokolování pro připojení ke koordinačnímu správci front. Alternativní konfigurace modulu protokolování viz “Alternativní konfigurace pro samostatný modul protokolování MFT” na stránce 770

Samostatný modul protokolování souborů není podporován na následujících platformách:

- z/OS z/OS
- IBM i IBM i

Postup

1. Ujistěte se, že máte nainstalovanou komponentu Managed File Transfer Logger . Další informace viz Volby produktu Managed File Transfer
2. Spusťte příkaz **fteCreateLogger** určující koordinačního správce front a nastavením parametru -loggerType na hodnotu `FILE` vytvořte samostatný modul protokolování souborů. Další informace viz fteCreateLogger.
3. Volitelné: Chcete-li použít vlastní formát, můžete upravit soubor XML vytvořený příkazem **fteCreateLogger** . Definice formátu protokolu je umístěna v souboru `FileLoggerFormat.xml` . Další informace viz téma “Formát samostatného modulu protokolování souborů MFT” na stránce 760.
4. Spusťte příkazy MQSC poskytnuté příkazem **fteCreateLogger** pro koordinačního správce front a vytvořte fronty modulu protokolování.
5. Identifikujte uživatele, který má spustit proces modulu protokolování, a nakonfigurujte pro tohoto uživatele oprávnění. Další informace viz téma “Konfigurace uživatelského přístupu pro samostatný modul protokolování souborů MFT” na stránce 765.
6. Volitelné: Samostatný modul protokolování souborů můžete dále konfigurovat úpravou souboru `logger.properties` vytvořeného při spuštění příkazu **fteCreateLogger** . Tento soubor je souborem vlastností Java , který se skládá z dvojic klíč-hodnota. Soubor `logger.properties` se nachází v adresáři *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/loggers/`*logger_name* . Další informace o dostupných vlastnostech a jejich dopadech naleznete v tématu MFT Vlastnosti konfigurace modulu protokolování.
7. Windows
   Volitelné: Pokud používáte systém Windows , můžete spustit samostatný modul protokolování souborů jako službu Windows . Spusťte příkaz **fteModifyLogger** s parametrem **-s** . Další informace viz fteModifyLogger.
8. Spusťte samostatný modul protokolování souborů pomocí příkazu **fteStartLogger** . Další informace viz fteStartLogger.

   Pokud jste provedli předchozí krok a použili jste příkaz **fteModifyLogger** s parametrem **-s** na systému Windows, spustí se samostatný modul protokolování souborů jako služba Windows .
9. Zkontrolujte výstup modulu protokolování. Samostatný modul protokolování souborů generuje dva typy výstupu: data auditu přenosu souborů a diagnostická data modulu protokolování. Data auditu přenosu souborů lze nalézt v adresáři *MQ_DATA_PATH*`/mqft/logs/`*coordination_qmgr_name*`/`

loggers/*logger_name*/logs. Diagnostická data modulu protokolování jsou k dispozici v adresáři *MQ_DATA_PATH*/mqft/logs/*coordination_qmgr_name*/loggers/*logger_name* .

10. Modul protokolování můžete zastavit pomocí příkazu **fteStopLogger** . Další informace viz fteStopLogger.

Výsledky

Související úlohy

“Konfigurace uživatelského přístupu pro samostatný modul protokolování souborů MFT” na stránce 765
V testovacím prostředí můžete přidat jakákoli nová oprávnění potřebná k vašemu běžnému uživatelskému účtu. V produkčním prostředí se doporučuje vytvořit nového uživatele s minimálními oprávněními potřebnými k provedení úlohy.

Související odkazy

Vlastnosti konfigurace modulu protokolování MFT

fteStartzapisovač protokolu

fteCreatezapisovač protokolu

fteModifyModul protokolování

fteStopModul protokolování

“Formát samostatného modulu protokolování souborů MFT” na stránce 760
Formát informací o zprávě zapsaných modulem protokolování souborů lze definovat v souboru FileLoggerFormat.xml .

Oprávnění pro zapisovač protokolu MFT

ALW *Formát samostatného modulu protokolování souborů MFT*

Formát informací o zprávě zapsaných modulem protokolování souborů lze definovat v souboru FileLoggerFormat.xml .

Konfigurační adresář pro modul protokolování je umístěn v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name*/loggers/*logger_name*. Při vytváření nového modulu protokolování souborů je vytvořena verze tohoto souboru, která obsahuje výchozí sadu definic používaných modulem protokolování souborů. Další informace o výchozí definici formátu protokolu viz MFT výchozí formát protokolu samostatného modulu protokolování souborů.

Chcete-li určit vlastní formát protokolu, upravte soubor FileLoggerFormat.xml .

Vlastní definice formátu protokolu

Definice formátu protokolu se skládá ze sady typů zpráv, přičemž každý typ zprávy má definici formátu. Definice formátu pro typ zprávy se skládá ze sady vložení poskytnutých ve formátu XPATH a oddělovače, který se používá k oddělení jednotlivých vložení. Pořadí vložení určuje pořadí, ve kterém je obsah umístěn do řádků generovaných pro výstup do souborů protokolu. Jedná se například o definici typu zprávy callStarted :

```
<callStarted>
  <format>
    <inserts>
      <insert type="user"   width="19" ignoreNull="false">/transaction/action/
       @time</insert>
      <insert type="user"   width="48" ignoreNull="false">/transaction/@ID</insert>
      <insert type="system" width="6"  ignoreNull="false">type</insert>
      <insert type="user"   width="0"  ignoreNull="false">/transaction/agent/
       @agent</insert>
      <insert type="user"   width="0"  ignoreNull="false">/transaction/agent/@QMgr</insert>
      <insert type="user"   width="0"  ignoreNull="false">/transaction/job/name</insert>
      <insert type="user"   width="0"  ignoreNull="true">/transaction/transferSet/
       call/command/@type</insert>
      <insert type="user"   width="0"  ignoreNull="true">/transaction/transferSet/
      call/command/@name</insert>
      <insert type="system" width="0"  ignoreNull="true">callArguments</insert>
    </inserts>
    <separator></separator>
```

```
  </format>
</callStarted>
```

Tento formát vytvoří řádek v souboru protokolu takto:

```
2011-11-25T10:53:04;414d5120514d5f67627468696e6b20206466cf4e20004f02;[CSTR];
  AGENT1;AGENT_QM;Managed Call;executable;echo;call test;
```

Vložení poskytnutá v definici formátu jsou v pořadí, ve kterém se informace objeví na řádku v souboru protokolu. Další informace o schématu XML definujícím formát souboru `FileLoggerFormat.xml` naleznete v tématu XSD formátu samostatného modulu protokolování souborů.

Typy zpráv

Agenti FTE zapisují rozsah různých typů zpráv do dílčího tématu SYSTEM.FTE/Log . Další informace viz SYSTEM.FTE téma. Definice souboru protokolu může obsahovat definice formátu pro tyto typy zpráv:

```
callCompleted
callStarted
monitorAction
monitorCreate
monitorFired
notAuthorized
scheduleDelete
scheduleExpire
scheduleSkipped
scheduleSubmitInfo
scheduleSubmitTransfer
scheduleSubmitTransferSet
transferStarted
transferCancelled
transferComplete
transferDelete
transferProgress
```

Formát zpráv se může lišit. Většina typů zpráv zapisuje jeden řádek do souboru protokolu pro každou zprávu protokolu spotřebovanou z dílčího tématu SYSTEM.FTE/Log . To vede k jednoduchému případu, kdy adresy XPATH poskytnuté v definici formátu protokolu souvisí s kořenem zprávy. Toto jsou typy zpráv, které používají tuto metodu pro zápis výstupu:

```
callCompleted
callStarted
monitorAction
monitorCreate
monitorFired
notAuthorized
scheduleDelete
scheduleExpire
scheduleSkipped
scheduleSubmitInfo
scheduleSubmitTransfer
transferStarted
transferCancelled
transferComplete
transferDelete
```

Jiná metoda použitá k zápisu zprávy protokolu používá více řádků k reprezentaci položek v sadě přenosu v rámci zprávy protokolu. V tomto případě se poskytnutý formát použije na každou položku v sadě přenosu v rámci zprávy protokolu. Chcete-li zahrnout informace, které jsou specifické pro každou položku v rámci sady přenosu, je nutné, aby poskytnutá proměnná XPATH používala položku jako svůj kořen XPATH. Toto jsou typy zpráv, které používají tuto metodu pro zápis výstupu:

```
scheduleSubmitTransferSet
transferProgress
```

Pro každou položku v sadě přenosu se zapíše řádek výstupu. Informace, které chcete opravit pro všechny položky v sadě přenosu, mohou i nadále používat adresy XPATH vzhledem ke kořenovému adresáři zprávy protokolu. V následujícím zjednodušeném příkladu definice formátu `transferProgress` je to časové razítko a ID přenosu, které jsou pevné. Jakékoli informace, které jsou relativní k položce jako její kořen, se budou lišit pro každý zapsaný řádek. V tomto příkladu jsou zapsány informace o zdrojovém a cílovém souboru pro každou položku.

```
<transferProgress>
      <format>
        <inserts>
          <insert type="user"   width="19" ignoreNull="false">/transaction/action/
           @time</insert>
          <insert type="user"   width="48" ignoreNull="false">/transaction/@ID</insert>
          <insert type="system" width="6"  ignoreNull="false">type</insert>
          <insert type="user"   width="3"  ignoreNull="true">status/@resultCode</insert>
          <insert type="user"   width="0"  ignoreNull="false">source/file |
           source/queue</insert>
          <insert type="user"   width="0"  ignoreNull="false">source/file/@size |
           source/queue/@size</insert>
          <insert type="user"   width="5"  ignoreNull="true">source/@type</insert>
          <insert type="user"   width="6"  ignoreNull="true">source/@disposition</insert>
          <insert type="user"   width="0"  ignoreNull="false">destination/file |
            destination/queue</insert>
          <insert type="user"   width="0"  ignoreNull="false">destination/file/@size |
            destination/queue/@size</insert>
          <insert type="user"   width="5"  ignoreNull="true">destination/@type</insert>
          <insert type="user"   width="9"  ignoreNull="true">destination/@exist</insert>
          <insert type="user"   width="0"  ignoreNull="true">status/supplement</insert>
        </inserts>
        <separator></separator>
      </format>
    </transferProgress>
```

Tím se vytvoří položka souboru protokolu jednoho nebo více řádků v tomto formátu:

```
2011-11-25T13:45:16;414d5120514d5f67627468696e6b20206466cf4e20033702;[TPRO];0
  ;/src/test1.file;3575;file;leave ;/dest/test1.file;3575;file;overwrite;;
2011-11-25T13:45:16;414d5120514d5f67627468696e6b20206466cf4e20033702;[TPRO];0
  ;/src/test2.file;3575;file;leave ;/dest/test2.file;3575;file;overwrite;;
```

Vložit formát

Při definování formátu pro typ zprávy jsou k dispozici dva typy vložení: `user` a `system`. Typ vložení je definován v atributu `type` prvku vložení. Oba typy vložení mohou mít také vlastní rozvržení pomocí atributů **`width`** a **`ignoreNull`** prvku vložení. Příklad:

```
<insert type="user" width="48" ignoreNull="false">/transaction/@ID</insert>
```

V tomto příkladu vložení vezme informace nalezené ve zprávě protokolu na adrese `/transaction/@ID` a ořízne je nebo vypíše na 48 znaků, než je zapíše do protokolu. Pokud má obsah `/transaction/@ID` hodnotu null, zapíše řetězec null po vyplnění na 48 znaků, protože atribut `ignoreNull` je nastaven na hodnotu `false`. Je-li parametr `ignoreNull` nastaven na hodnotu `true` , bude místo toho zapsán prázdný řetězec, vyplněný na 48 znaků. Nastavení width="0 " znamená, že šířka sloupce není oříznuta, neznamená to, že je šířka oříznuta na 0. Atribut `ignoreNull` lze tímto způsobem použít ke zjištění v protokolu, když je nalezena hodnota null, když nebyla očekávána. To může být užitečné při ladění nové definice souboru protokolu.

Uživatelem definované vložení

Uživatelská vložka obsahuje adresu XPATH pro informace, které mají být v dané vložení zapsány. Tato adresa odkazuje na informaci nalezenou ve zprávě protokolu FTE. Další informace o formátech zpráv protokolu viz:

- Formát zpráv protokolu přenosu souborů
- Formáty zpráv protokolu naplánovaného přenosu souborů

- Formát zprávy protokolu monitoru MFT

Vložení definovaná systémem

Vložení definovaná systémem obsahují klíčové slovo, které odkazuje na informaci, kterou nelze nalézt ve zprávě protokolu, nebo ji nelze snadno definovat pomocí jazyka XPATH.

Podporované systémové vložky jsou:

- `type` -Zapíše typ zprávy protokolu v krátkém formátu.
- `callArguments` -Zapíše sadu argumentů dodaných spravovanému volání ve formátu odděleném mezerami.
- `transferMetaData` -Zapíše sadu položek metadat definovaných pro přenos ve formátu *klíč=hodnota* oddělený čárkami.

V následující tabulce je uvedena hodnota "type" pro vložení definovaná systémem pro každý typ zprávy.

Tabulka 50. Souhrn podporovaných typů zpráv a jejich vložení do systému "type".

Typ zprávy	**Hodnota systémové vložky "type"**
callCompleted	[CCOM]
callStarted	[CSTR]
monitorAction	[MACT]
monitorCreate	[MCRT]
monitorFired	[MFIR]
notAuthorized	[AUTH]
scheduleDelete	[SDEL]
scheduleExpire	[SEXP]
scheduleSkipped	[SSKP]
scheduleSubmitInformace	[SSIN]
scheduleSubmitTransfer	[SSTR]
scheduleSubmitTransferSet	[SSTS]
transferStarted	[TSTR]
transferCancelled	[TCAN]
transferComplete	[TCOM]
transferDelete	[TDEL]
transferProgress	[TPRO]

Související odkazy

Výchozí formát protokolu samostatného modulu protokolování souborů MFT

XSD formátu samostatného modulu protokolování souborů
SYSTEM.FTE
Formáty zpráv protokolu přenosu souborů
Formáty zpráv protokolu naplánovaného přenosu souborů
Formát zprávy protokolu monitoru MFT

ALW *Vyloučení typů zpráv ze samostatného modulu protokolování souborů MFT*
Chcete-li vyloučit určitý typ zprávy z výstupu modulu protokolování souborů, můžete použít prázdné prvky typu zprávy.

Příklad

Například následující definice formátu zastaví výstup zpráv `transferProgress` zapisovače protokolu souborů.

```
<?xml version="1.0" encoding="UTF-8"?>
<logFormatDefinition  xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance" version="1.00"
 xsi:noNamespaceSchemaLocation="FileLoggerFormat.xsd">
  <messageTypes>
    <transferProgress></transferProgress>
  </messageTypes>
</logFormatDefinition>
```

ALW *Definování vlastních formátů pro samostatný modul protokolování souborů MFT*
Je možné definovat podmnožinu vlastních typů zpráv v rámci definice formátu protokolu, abyste snížili množství konfigurace potřebné k přizpůsobení formátu souboru protokolu.

Informace o této úloze

Pokud není prvek `messageTypes` zahrnut v souboru `FileLoggerFormat.xml` , formát pro tento typ zprávy použije výchozí formát. Musíte pouze určit formáty, které se mají lišit od výchozích.

Příklad

V tomto příkladu definice formátu nahradí výchozí formát pro typ zprávy `transferStarted` s touto sníženou verzí, která bude výstupem pouze uživatel, který spustil přenos. Všechny ostatní typy zpráv používají výchozí formát, protože nejsou zahrnuty v této definici formátu protokolu:

```
<?xml version="1.0" encoding="UTF-8"?>
<logFormatDefinition  xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance" version="1.00"
 xsi:noNamespaceSchemaLocation="FileLoggerFormat.xsd">
  <messageTypes>
    <transferStarted>
      <format>
        <inserts>
          <insert type="user"   width="19" ignoreNull="false">/transaction/action/
           @time</insert>
          <insert type="user"   width="48" ignoreNull="false">/transaction/@ID</insert>
          <insert type="system" width="6"  ignoreNull="false">type</insert>
          <insert type="user"   width="0"  ignoreNull="true">/transaction/originator/
           userID</insert>
        </inserts>
        <separator>;</separator>
      </format>
    </transferStarted>
  </messageTypes>
</logFormatDefinition>
```

Související odkazy

Výchozí formát protokolu samostatného modulu protokolování souborů MFT
XSD formátu samostatného modulu protokolování souborů

ALW *Snížení počtu duplicitních zpráv v samostatném modulu protokolování souborů MFT*
V protokolu samostatného modulu protokolování souborů se mohou vyskytnout duplicitní zprávy protokolu. Pomocí souboru `logger.properties` můžete vyladit samostatný modul protokolování souborů a snížit počet duplikátů.

Duplicitní zprávy v protokolu modulu protokolování souborů

V případě selhání může být zpráva protokolu zapsána do protokolu samostatného modulu protokolování souborů bez spotřeby zprávy protokolu ze systému SYSTEM.FTE/Log# téma potvrzováno pro IBM MQ. Pokud k tomu dojde, když se samostatný modul protokolování souborů restartuje, znovu načte stejnou zprávu a znovu ji zapíše do souboru protokolu. Plánujte zvládnout možnost těchto duplikátů při pohledu na soubory protokolu buď ručně, nebo při jejich automatickém zpracování. Pro usnadnění detekce duplikátů je při spuštění samostatného zapisovače protokolu do souboru protokolu vygenerována následující zpráva:

```
BFGDB0054I: The file logger has successfully started
```

Duplikáty se vždy vyskytují kolem času zahájení samostatného modulu protokolování souborů, protože se jedná o zpracování poslední zprávy přečtené před selháním předchozí instance. Tím, že zjistíte, kdy byla spuštěna nová instance, můžete zjistit, zda by měly být očekávány duplicitní položky a zda je třeba je zpracovat či nikoli.

Snížení počtu duplikátů

Samostatný modul protokolování souborů seskupuje zprávy protokolu, které zpracovává, do transakcí, aby zlepšil výkon. Tato velikost dávky je maximální počet duplicitních zpráv, které můžete vidět v případě selhání. Chcete-li snížit počet duplikátů, můžete vyladit následující vlastnost v souboru `logger.properties` :

```
wmqfte.max.transaction.messages
```

Například nastavením této hodnoty na hodnotu 1 se maximální počet duplicitních zpráv sníží na hodnotu 1. Mějte na paměti, že úprava této hodnoty má vliv na výkon samostatného modulu protokolování souborů, takže je nutné provést důkladné testování, aby nedošlo k nepříznivému ovlivnění systému.

Soubor `logger.properties` se nachází v adresáři *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/loggers/`*logger_name* . Další informace o dostupných vlastnostech a jejich účincích viz MFT vlastnosti konfigurace modulu protokolování

ALW ***Konfigurace uživatelského přístupu pro samostatný modul protokolování souborů MFT***
V testovacím prostředí můžete přidat jakákoli nová oprávnění potřebná k vašemu běžnému uživatelskému účtu. V produkčním prostředí se doporučuje vytvořit nového uživatele s minimálními oprávněními potřebnými k provedení úlohy.

Informace o této úloze

Samostatný modul protokolování souborů a produkt IBM MQ musíte nainstalovat na jeden systém. Nakonfigurujte oprávnění uživatele takto:

Postup

1. Ujistěte se, že uživatel má oprávnění ke čtení a v případě potřeby ke spouštění souborů instalovaných v rámci instalace produktu Managed File Transfer .

2. Ujistěte se, že uživatel má oprávnění k vytvoření a zápisu do libovolného souboru v adresáři `logs` , který je v konfiguračním adresáři. Tento adresář se používá pro protokol událostí a v případě potřeby pro diagnostické trasování a soubory FFDC (First Failure Data Capture).
3. Ujistěte se, že uživatel má svou vlastní skupinu a není také ve skupinách s rozsáhlými oprávněními pro koordinačního správce front. Uživatel by neměl být ve skupině mqm. Na některých platformách je skupině personálu automaticky také udělen přístup ke správci front; samostatný uživatel modulu protokolování souborů by neměl být ve skupině personálu. Záznamy oprávnění pro samotného správce front a pro objekty v něm můžete zobrazit pomocí konzoly IBM MQ Explorer. Klepněte pravým tlačítkem myši na objekt a vyberte volbu **Oprávnění k objektu > Spravovat záznamy oprávnění**. Na příkazovém řádku můžete použít příkazy dspmqaut (oprávnění k zobrazení) nebo dmpmqaut (oprávnění k výpisu paměti).
4. Pomocí okna **Spravovat záznamy oprávnění** v souboru IBM MQ Explorer nebo příkazu setmqaut (udělit nebo odebrat oprávnění) můžete přidat oprávnění pro vlastní skupinu uživatele (v systému AIXjsou oprávnění systému IBM MQ přidružena pouze ke skupinám, nikoli jednotlivým uživatelům). Požadované orgány jsou tyto:
   - Připojte se a informujte se o správci front (knihovny produktu IBM MQ Java vyžadují oprávnění k dotazování).
   - Přihlaste se k odběru oprávnění v systému SYSTEM.FTE .
   - Zadejte oprávnění do SYSTEM.FTE.LOG.RJCT. Fronta*logger_name* .
   - Získejte oprávnění k systému SYSTEM.FTE.LOG.CMD. fronta*logger_name* .

   Zadané názvy front odmítnutí a příkazů jsou předvolené názvy. Pokud jste při konfiguraci samostatných front modulu protokolování vybrali různé názvy front, přidejte oprávnění k těmto názvům front.

Instalace samostatného modulu protokolování databáze MFT

Chcete-li nainstalovat a nakonfigurovat samostatný modul pro protokolování databáze, postupujte takto.

Informace o této úloze

Důležité: Moduly protokolování Managed File Transfer nejsou na platformě IBM i podporovány.

Další informace o modulu protokolování samostatné databáze naleznete v části “Konfigurace modulu protokolování MFT” na stránce 757.

Poznámka: Nelze spustit více než jeden modul pro protokolování databáze (samostatně nebo Java EE) pro stejné schéma v databázi současně. Pokus o provedení této operace by měl za následek kolize při pokusu o zápis dat protokolu přenosu do databáze.

Postup

1. Nainstalujte databázový software pomocí dokumentace pro vaši databázi.

   Pokud je podpora JDBC volitelnou komponentou pro vaši databázi, musíte tuto komponentu nainstalovat.
2. Spuštěním příkazu **`fteCreateLogger`** s nastavením parametru **`-loggerType`** na hodnotu DATABASE vytvořte samostatný modul pro protokolování databáze. Další informace viz fteCreateLogger.

   Výchozí název schématu je FTELOG. Pokud použijete jiný název schématu než FTELOG, musíte upravit poskytnutý soubor SQL odpovídající vaší databázi, `ftelog_tables_db2.sql` nebo `ftelog_tables_oracle.sql`, aby odrážel tento název schématu, než budete pokračovat dalším krokem. Další informace viz wmqfte.database.schema v části MFT vlastnosti konfigurace modulu protokolování.
3. Vytvořte požadované databázové tabulky pomocí nástrojů databáze.

   Multi V systému Multiplatformssoubory `ftelog_tables_db2.sql` a `ftelog_tables_oracle.sql` obsahují příkazy SQL, které můžete spustit pro vytvoření tabulek.

z/OS V systému z/OSzávisí soubor, který potřebujete spustit, na verzi produktu Db2 for z/OS , kterou používáte:

- Pro systém Db2 for z/OS 9.0 a dřívější spusťte soubor `ftelog_tables_zos.sql` a vytvořte tabulky. Tento soubor vytvoří tabulky pomocí datového typu INTEGER pro pole, která označují velikosti přenášených souborů a ID tabulky přidružené ke každému přenosu.
- Pro systém Db2 for z/OS 9.1 a novější spusťte soubor `ftelog_tables_zos_bigint.sql` a vytvořte tabulky. Tento soubor vytvoří tabulky pomocí datového typu BIGINT pro pole, která označují velikost přenášených souborů a ID tabulky přidružené ke každému přenosu.

4. Spusťte příkazy MQSC poskytované příkazem **fteCreateLogger** pro správce front příkazů modulu protokolování, abyste vytvořili fronty modulu protokolování. Samostatný modul pro protokolování databáze používá dvě fronty v koordinačním správci front. První fronta je fronta příkazů, ve které jsou umístěny zprávy pro řízení činnosti samostatného modulu pro protokolování databáze. Výchozí název této fronty příkazů je SYSTEM.FTE.LOG.CMD.*název_logger_name*. Druhá fronta je fronta odmítnutí. Protože samostatný modul pro protokolování databáze nikdy nezahazuje zprávy protokolu, pokud modul pro protokolování narazí na zprávu, kterou nemůže zpracovat, umístí zprávu do fronty odmítnutí k prozkoumání a možnému opětovnému zpracování. Nedoporučuje se k tomuto účelu používat frontu nedoručených zpráv správce front, protože odmítnuté zprávy nemají záhlaví DLH a odmítnuté zprávy by z jiných důvodů neměly být kombinovány se zprávami vloženými do fronty nedoručených zpráv. Výchozí název fronty odmítnutí je SYSTEM.FTE.LOG.RJCT.*název_logger_name*. Tyto dvě fronty jsou definovány ve skriptových souborech MQSC generovaných příkazem **fteCreateLogger** .
5. Zvolte uživatele a nakonfigurujte oprávnění
6. Volitelné: Modul pro protokolování samostatné databáze můžete dále konfigurovat úpravou souboru `logger.properties` vytvořeného příkazem **fteCreateLogger** v kroku “2” na stránce 766. Tento soubor je souborem vlastností Java , který se skládá z dvojic klíč-hodnota. Soubor `logger.properties` se nachází v adresáři *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/loggers/`*logger_name* . Další informace o dostupných vlastnostech a jejich účincích naleznete v tématu MFT Vlastnosti konfigurace modulu protokolování.
7. Windows
   Volitelné: Používáte-li systém Windows , můžete modul protokolování samostatné databáze spustit jako službu systému Windows . Spusťte příkaz **fteModifyLogger** s parametrem **-s** . Další informace viz fteModifyLogger.
8. Volitelné: Pokud používáte databázi Oracle nebo se vzdáleně připojujete k databázi Db2 , budete muset zadat jméno uživatele a heslo, které modul protokolování použije k ověření s databázovým serverem. Toto jméno uživatele a heslo je uvedeno v souboru pověření, který odpovídá formátu definovanému schématem `MQMFTCredentials.xsd` . Další informace viz Formát souboru pověření MFT. Po vytvoření souboru pověření musíte zadat umístění souboru pověření v souboru `logger.properties` pomocí vlastnosti `wmqfte.database.credentials.file` .
9. Spusťte samostatný modul pro protokolování databáze pomocí příkazu **fteStartLogger** . Standardně je samostatný modul pro protokolování databáze spuštěn na pozadí a samostatný modul pro protokolování databáze umístí výstup do souboru v adresáři `logs` . Chcete-li spustit modul protokolování samostatné databáze v popředí a vytvořit výstup do konzoly i do souboru protokolu, přidejte do příkazu **fteStartLogger** parametr **-F** .

   Pokud jste provedli předchozí krok a použili jste příkaz **fteModifyLogger** s parametrem **-s** v systému Windows, spustí se samostatný modul pro protokolování databáze jako služba Windows .

Související úlohy

“Konfigurace uživatelského přístupu pro samostatný modul pro protokolování databáze MFT” na stránce 768

V testovacím prostředí můžete přidat jakákoli nová oprávnění potřebná k vašemu běžnému uživatelskému účtu. V produkčním prostředí se doporučuje vytvořit nového uživatele s minimálními oprávněními potřebnými k provedení úlohy.

Související odkazy

Vlastnosti konfigurace modulu protokolování MFT

fteStartzapisovač protokolu
fteModifyModul protokolování
Oprávnění pro zapisovač protokolu MFT

Použití MFT se vzdálenou databází

Modul protokolování Managed File Transfer můžete použít ke komunikaci s databází na vzdáleném systému.

Informace o této úloze

Máte-li nainstalovanou databázi na jiném počítači, než na kterém je nainstalován počítač Managed File Transfer , postupujte takto. Pokud není uvedeno jinak, platí tento postup pro databázi Db2 i pro databázi Oracle .

Postup

1. Nainstalujte databázového klienta na systém, na kterém jste nainstalovali produkt Managed File Transfer .
2. Přidejte vzdálený databázový server do konfigurace lokálního databázového klienta. Tato aktualizace konfigurace je potřebná, aby produkt Managed File Transfer a IBM MQ správně přistoupily k databázi.
3. Zadejte nové vlastnosti v souboru `logger.properties` pro připojení k databázi pomocí souboru pověření: **`wmfte.database.credentials.file`**.

   Poznámka: Deprecated Dřívější verze produktu Managed File Transfer používaly vlastnosti **`wmqfte.oracle.user`** nebo **`wmqfte.database.user`**a **`wmqfte.oracle.password`** nebo **`wmqfte.database.password`**. Tyto vlastnosti jsou nyní zamítnuty. Místo toho použijte **`wmfte.database.credentials.file`** .
4. **Oracle :** Chcete-li povolit vzdálené připojení k databázi, změňte sekci XAResourceManager v souboru `qm.ini` koordinačního správce front na následující (ujistěte se, že jste změnili název databáze, jméno uživatele a heslo uživatele tak, aby odpovídaly vašim vlastním informacím):

   `Oracle_XA+Acc=P/ftelog/qgw783jhT+SesTm=35+DB=FTEAUDIT1`**`+SqlNet=FTEAUDIT1`**`+threads=false`,
   změna je zvýrazněna tučným písmem.
5. **Oracle :** Zadejte hostitele a port v souboru `logger.properties` pomocí vlastností **`wmqfte.oracle.host`** a **`wmqfte.oracle.port`** . Výchozí hodnoty pro hostitele a port vám umožňují pracovat s lokálním databázovým klientem, takže pokud jste dříve pracovali s lokální databází, možná jste tyto hodnoty nenastavili.

Související odkazy

Vlastnosti konfigurace modulu protokolování MFT

Konfigurace uživatelského přístupu pro samostatný modul pro protokolování databáze MFT

V testovacím prostředí můžete přidat jakákoli nová oprávnění potřebná k vašemu běžnému uživatelskému účtu. V produkčním prostředí se doporučuje vytvořit nového uživatele s minimálními oprávněními potřebnými k provedení úlohy.

Informace o této úloze

Počet a typ uživatelských účtů, které potřebujete ke spuštění samostatného modulu pro protokolování databáze, závisí na počtu používaných systémů. Samostatný modul protokolování databáze IBM MQ a vaši databázi můžete nainstalovat na jeden systém nebo na dva systémy. Samostatný modul pro protokolování databáze musí být ve stejném systému jako IBM MQ. Komponenty lze instalovat v následujících topologiích:

Samostatný zapisovač protokolu databáze IBM MQ a databáze na stejném systému
Můžete definovat jednoho uživatele operačního systému pro použití se všemi třemi komponentami. Jedná se o vhodnou konfiguraci pro samostatný modul pro protokolování databáze. Samostatný modul pro protokolování databáze používá režim vazeb pro připojení k produktu IBM MQ a nativní připojení pro připojení k databázi.

Samostatný zapisovač protokolu databáze a IBM MQ na jednom systému, databáze na odděleném systému
Pro tuto konfiguraci vytvoříte dva uživatele: uživatele operačního systému v systému, na kterém je spuštěn samostatný modul pro protokolování databáze, a uživatele operačního systému se vzdáleným přístupem k databázi na databázovém serveru. Jedná se o vhodnou konfiguraci pro modul pro protokolování samostatné databáze s použitím vzdálené databáze. Samostatný modul pro protokolování databáze používá režim vazeb pro připojení k produktu IBM MQ a připojení klienta pro přístup k databázi.

Jako příklad zbytek těchto pokynů předpokládá, že se uživatel nazývá `ftelog`, ale můžete použít libovolné jméno uživatele. Nakonfigurujte oprávnění uživatele takto:

Postup

1. Ujistěte se, že uživatel má oprávnění ke čtení a v případě potřeby ke spouštění souborů instalovaných v rámci instalace Vzdálené nástroje a dokumentace Managed File Transfer .
2. Ujistěte se, že uživatel má oprávnění k vytvoření a zápisu do libovolného souboru v adresáři `logs` (v konfiguračním adresáři). Tento adresář se používá pro protokol událostí a v případě potřeby pro diagnostické trasování a soubory FFDC.
3. Ujistěte se, že uživatel má svou vlastní skupinu a není také ve skupinách s rozsáhlými oprávněními pro koordinačního správce front. Uživatel by neměl být ve skupině mqm. Na určitých platformách je skupině personálu také automaticky udělen přístup ke správci front; samostatný uživatel modulu protokolování databáze by neměl být ve skupině personálu. Pomocí konzoly IBM MQ Explorermůžete zobrazit záznamy oprávnění pro samotného správce front a pro objekty v něm obsažené. Klepněte pravým tlačítkem myši na objekt a vyberte volbu **Oprávnění k objektu > Spravovat záznamy oprávnění**. Na příkazovém řádku můžete použít příkazy dspmqaut (oprávnění k zobrazení) nebo dmpmqaut (oprávnění k výpisu paměti).
4. Pomocí okna **Spravovat záznamy oprávnění** v souboru IBM MQ Explorer nebo příkazu setmqaut (udělit nebo odebrat oprávnění) můžete přidat oprávnění pro vlastní skupinu uživatele (v systému AIXjsou oprávnění systému IBM MQ přidružena pouze ke skupinám, nikoli jednotlivým uživatelům). Požadované orgány jsou tyto:
   - Připojte se a informujte se o správci front (knihovny produktu IBM MQ Java vyžadují oprávnění k dotazování).
   - Přihlaste se k odběru oprávnění v systému SYSTEM.FTE .
   - Zadejte oprávnění do SYSTEM.FTE.LOG.RJCT. Fronta*logger_name* .
   - Získejte oprávnění k systému SYSTEM.FTE.LOG.CMD. fronta*logger_name* .

   Zadané názvy front odmítnutí a příkazů jsou předvolené názvy. Pokud jste při konfiguraci samostatných front modulu protokolování databáze vybrali jiné názvy front, přidejte oprávnění k těmto názvům front.
5. Proveďte konfiguraci uživatele, která je specifická pro databázi, kterou používáte.
   - Pokud je vaše databáze Db2, postupujte takto:

     Existuje několik mechanizmů pro správu uživatelů databáze s produktem Db2. Tyto pokyny se vztahují na výchozí schéma založené na uživatelích operačního systému.

     – Ujistěte se, že uživatel `ftelog` není v žádné skupině administrace Db2 (například db2iadm1, db2fadm1nebo dasadm1).
     – Udělte uživateli oprávnění pro připojení k databázi a oprávnění k výběru, vložení a aktualizaci tabulek, které jste vytvořili v rámci kroku 2: vytvoření požadovaných databázových tabulek .
   - Pokud je vaše databáze Oracle, postupujte takto:

- Ujistěte se, že uživatel `ftelog` není v žádné skupině administrace Oracle (například ora_dba na Windows nebo dba na AIX and Linux)
- Udělte uživateli oprávnění pro připojení k databázi a oprávnění k výběru, vložení a aktualizaci tabulek, které jste vytvořili v rámci kroku 2: vytvoření požadovaných databázových tabulek .

Alternativní konfigurace pro samostatný modul protokolování MFT

Samostatný modul protokolování Managed File Transfer , ať už se jedná o typ souboru nebo databáze, se obvykle nachází ve stejném systému jako koordinační správce front a je připojen ke koordinačnímu správci front v režimu vazeb IBM MQ . Lze jej však také nainstalovat na stejný systém jako správce front, který má konektivitu ke koordinačnímu správci front. Samostatný modul protokolování přijímá zprávy pomocí odběru, který samostatný modul protokolování vytváří automaticky. Toto je konfigurace popsaná v pokynech k instalaci.

Máte-li však aspekty specifické pro konkrétní server, můžete nakonfigurovat samostatný modul protokolování tak, aby přijímal zprávy dvěma dalšími způsoby řízenými vlastností wmqfte.message.source.type . Tato vlastnost je popsána v části MFT Vlastnosti konfigurace modulu protokolování.

Administrativní odběr

Při výchozím nastavení vytvoří samostatný modul protokolování vlastní odběr systému SYSTEM.FTE/Log/# s použitím výchozích voleb trvalého odběru a spravovaného odběru (tj. správce front řídí záložní frontu používanou k uchování zpráv před jejich předáním aplikaci). Pokud jsou pro odběr nebo frontu vyžadovány další volby, můžete místo toho vytvořit odběr sami, nastavit požadované volby a nakonfigurovat samostatný modul protokolování tak, aby místo toho používal tento odběr. Nezapomeňte přidat oprávnění pro samostatný modul protokolování k použití vytvořeného odběru.

Příkladem použití této konfigurace je rozdělit protokolovací prostor pomocí dvou odběrů se zástupnými znaky, odeslat protokoly z agentů, jejichž název začíná na FINANCE, do jedné databáze a protokoly z agentů začínajících na ACCOUNTING do jiné. Tento typ konfigurace vyžaduje dvě samostatné instance modulu protokolování, každou s vlastním souborem `logger.properties` odkazujícím na požadovaný odběr a vlastní frontu příkazů a frontu odmítnutí.

Chcete-li shromažďovat zprávy protokolu pouze od agentů, jejichž názvy začínají řetězcem ACCOUNTING, vytvořte objekt odběru v koordinačním správci front s řetězcem tématu SYSTEM.FTE/Log/ACCOUNTING*. Nastavte hodnotu **Použití zástupného znaku** na **zástupný znak na úrovni znaku**. Musíte také přidat položky do souboru `logger.properties` pro váš modul protokolování. Pokud například vytvoříte objekt odběru s názvem ACCOUNTING.LOGS s těmito nastaveními přidejte do souboru `logger.properties` následující položky:

```
wmqfte.message.source.type=administrative subscription
wmqfte.message.source.name=ACCOUNTING.LOGS
```

Samostatný modul protokolování zpracovává zprávy protokolu, které začínají řetězcem tématu SYSTEM.FTE/Log/ . Můžete zadat více omezující řetězec tématu, ale nemůžete zadat méně omezující řetězec. Zadáte-li méně omezující řetězec s chybou, všechna publikování související s jiným řetězcem tématu než SYSTEM.FTE/Log/ přejděte do fronty odmítnutí a samostatný zapisovač protokolu vytvoří chybovou zprávu BFGDB0002E. Tato chybová zpráva znamená, že došlo k problému s konfigurací samostatného modulu protokolování.

Fronta

Typickou topologií je místo, kde je samostatný modul protokolování spuštěn ve stejném systému jako koordinační správce front. Pokud to není možné, můžete vytvořit odběr v koordinačním správci front s použitím fronty v jiném správci front jako cíle odběru (buď pomocí definice vzdálené fronty, nebo pomocí vlastnosti DESTQMGR odběru). Modul protokolování pak může být spuštěn v systému, který je hostitelem druhého správce front, a číst zprávy z fronty. Chcete-li zajistit integritu transakcí, musí se samostatný modul protokolování vždy připojit ke svému správci front v režimu vazeb. Frontu odmítnutí a frontu příkazů

musíte definovat ve stejném správci front, ke kterému se připojuje samostatný modul protokolování. Správci front musí být ve verzi IBM WebSphere MQ 7.5 nebo novější.

Například, chcete-li shromáždit zprávy protokolu, které jsou umístěny do fronty USER.QUEUE pomocí odběru, přidejte tyto položky do souboru `logger.properties` :

```
wmqfte.message.source.type=queue
wmqfte.message.source.name=USER.QUEUE
```

Instalace modulu protokolování databáze Java EE pro MFT

Při instalaci a konfiguraci modulu protokolování databáze JEE pro použití s produktem Managed File Transferpostupujte podle těchto pokynů.

Informace o této úloze

Další informace o modulu protokolování databáze Java EE naleznete v tématu “Konfigurace modulu protokolování MFT” na stránce 757.

Poznámka: Modul protokolování databáze Java EE nelze spustit současně se samostatným modulem protokolování, pokud tyto moduly protokolování nepoužívají samostatné instance databáze.

Postup

1. Před instalací modulu protokolování databáze Java EE je třeba připravit prostředí. Postupujte podle pokynů v tématu “Příprava na instalaci modulu protokolování databáze Java EE pro MFT” na stránce 772.
2. Nainstalujte modul protokolování databáze Java EE do aplikačního serveru kompatibilního s Java Platform, Enterprise Edition (Java EE) nebo Jakarta EE .

   Pokyny viz “Instalace modulu protokolování databáze Java EE pro MFT pomocí WebSphere Application Server traditional 9.0” na stránce 774

Související úlohy

“Příprava na instalaci modulu protokolování databáze Java EE pro MFT” na stránce 772
Před instalací modulu pro protokolování databáze Java EE postupujte podle těchto pokynů a připravte prostředí Managed File Transfer .

“Instalace modulu protokolování databáze Java EE pro MFT pomocí WebSphere Application Server traditional 9.0” na stránce 774
Při instalaci a konfiguraci modulu pro protokolování databáze Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s operačním systému WebSphere Application Server traditional 9.0postupujte podle těchto pokynů.

“Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro MFT” na stránce 779
Při konfiguraci modulu protokolování databáze Java Platform, Enterprise Edition (Java EE) pro systém Managed File Transferpotřebujete uživatelské účty pro přístup k produktu IBM MQ, k databázi a k operačnímu systému. Počet požadovaných uživatelů operačního systému závisí na počtu systémů, které používáte k hostování těchto komponent.

“Migrace ze samostatného modulu pro protokolování databáze na modul pro protokolování databáze Java EE pro MFT” na stránce 780
Můžete provést migraci ze samostatného modulu pro protokolování databáze do modulu pro protokolování databáze Java EE . Musíte zastavit samostatný modul pro protokolování databáze a nainstalovat modul pro protokolování databáze JEE. Chcete-li zabránit ztrátě nebo duplikaci položek protokolu, musíte před zastavením samostatného modulu pro protokolování databáze zastavit publikování zpráv v tématu SYSTEM.FTE a po instalaci modulu pro protokolování databáze Java EE jej znovu spustit. Před migrací zálohujte databázi.

Související odkazy

Oprávnění pro zapisovač protokolu MFT

Příprava na instalaci modulu protokolování databáze Java EE pro MFT

Před instalací modulu pro protokolování databáze Java EE postupujte podle těchto pokynů a připravte prostředí Managed File Transfer .

Informace o této úloze

Další informace o modulu protokolování databáze Java EE naleznete v tématu “Konfigurace modulu protokolování MFT” na stránce 757.

Postup

1. Nainstalujte databázový software pomocí dokumentace pro vaši databázi.

   Pokud je podpora JDBC volitelnou komponentou pro vaši databázi, musíte tuto komponentu nainstalovat.
2. Vytvořte databázi pomocí nástrojů, které poskytuje vaše databáze. Databáze musí mít tabulkový prostor a velikost stránky fondu vyrovnávacích pamětí alespoň 8K.

   Výchozí název schématu je FTELOG. Pokud použijete jiný název schématu než FTELOG, musíte upravit poskytnutý soubor SQL odpovídající vaší databázi, `ftelog_tables_db2.sql` nebo `ftelog_tables_oracle.sql`, aby to odráželo, než budete pokračovat dalším krokem.

   Poznámka: Soubory `ftelog_tables_db2.sql` a `ftelog_tables_oracle.sql` jsou v cestě k souboru `<MQ-installation-path>/mqft/sql`
3. Vytvořte požadované databázové tabulky pomocí nástrojů databáze.

   Multi V systému Multiplatformssoubory `ftelog_tables_db2.sql` a `ftelog_tables_oracle.sql` obsahují příkazy SQL, které můžete spustit pro vytvoření tabulek.

   z/OS V systému z/OSzávisí soubor, který potřebujete spustit, na verzi produktu Db2 for z/OS , kterou používáte:

   - Pro systém Db2 for z/OS 9.0 a dřívější spusťte soubor `ftelog_tables_zos.sql` a vytvořte tabulky. Tento soubor vytvoří tabulky pomocí datového typu INTEGER pro pole, která označují velikosti přenášených souborů a ID tabulky přidružené ke každému přenosu.
   - Pro systém Db2 for z/OS 9.1 a novější spusťte soubor `ftelog_tables_zos_bigint.sql` a vytvořte tabulky. Tento soubor vytvoří tabulky pomocí datového typu BIGINT pro pole, která označují velikost přenášených souborů a ID tabulky přidružené ke každému přenosu.
4. Pokud jste změnili název schématu z FTELOG, musíte změnit název schématu v souboru EAR. Další informace viz “Změna názvu schématu v modulu protokolování databáze Java EE pro MFT” na stránce 773.
5. Vytvořte frontu odmítnutí v adresáři IBM MQ.

   Protože modul protokolování nikdy nezahazuje zprávy protokolu, pokud modul protokolování narazí na zprávu, kterou nemůže zpracovat, umístí zprávu do fronty odmítnutí k prozkoumání a možnému opětovnému zpracování. K tomuto účelu nepoužívejte frontu nedoručených zpráv správce front, protože odmítnuté zprávy nemají záhlaví DLH a odmítnuté zprávy nesmí být z jiných důvodů kombinovány se zprávami vloženými do fronty nedoručených zpráv. Příkaz **`fteCreateLogger`** vytvoří frontu odmítnutí. Výchozí název této fronty odmítnutí je SYSTEM.FTE.LOG.RJCT.*název_protokolu*
6. Postupujte podle pokynů v tématu “Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro MFT” na stránce 779.

Jak pokračovat dále

Nainstalujte modul protokolování databáze Java EE do aplikačního serveru kompatibilního s produktem Java EE nebo Jakarta EE . Postupujte podle pokynů v části “Instalace modulu protokolování databáze Java EE pro MFT pomocí WebSphere Application Server traditional 9.0” na stránce 774

Změna názvu schématu v modulu protokolování databáze Java EE pro MFT

Modul pro protokolování databáze Java Platform, Enterprise Edition (Java EE) může používat databázi, která má jiný než výchozí název schématu. Musíte změnit název schématu v souboru EAR modulu pro protokolování databáze Java EE .

Informace o této úloze

Chcete-li změnit název schématu, které používá modul pro protokolování databáze Java EE , postupujte takto:

Postup

1. Extrahujte soubor JAR JPA ze souboru EAR pomocí následujícího příkazu:

   ```
   jar -xvf ear_file lib/jpa_file
   ```

   kde:

   - *soubor_do uší* je `com.ibm.wmqfte.databaselogger.jee.oracle.ear` nebo `com.ibm.wmqfte.databaselogger.jee.ear` v závislosti na tom, zda používáte databázi Db2 nebo Oracle.
   - *soubor_jpa_file* je `com.ibm.wmqfte.web.jpa.oracle.jar` nebo `com.ibm.wmqfte.web.jpa.jar` v závislosti na tom, zda používáte databázi Db2 nebo Oracle.
2. Extrahujte soubor `persistence.xml` ze souboru JAR JPA pomocí následujícího příkazu:

   ```
   jar -xvf lib/jpa_file META_INF/persistence.xml
   ```

   kde:

   - *soubor_jpa_file* je `com.ibm.wmqfte.web.jpa.oracle.jar` nebo `com.ibm.wmqfte.web.jpa.jar` v závislosti na tom, zda používáte databázi Db2 nebo Oracle.
3. Upravte soubor `persistence.xml` a změňte následující řádek:

   ```
   <property name="openjpa.jdbc.Schema" value="schema_name" />
   ```

   kde:

   - *název_schématu* je název schématu, které chcete použít.
4. Aktualizujte soubor JAR JPA pomocí upraveného souboru `persistence.xml` pomocí následujícího příkazu:

   ```
   jar -uvf lib/jpa_file META_INF/persistence.xml
   ```

   kde:

   - *soubor_jpa_file* je `com.ibm.wmqfte.web.jpa.oracle.jar` nebo `com.ibm.wmqfte.web.jpa.jar` v závislosti na tom, zda používáte databázi Db2 nebo Oracle.
5. Aktualizujte soubor EAR pomocí upraveného souboru JAR JPA pomocí následujícího příkazu:

   ```
   jar -uvf ear_file lib/jpa_file
   ```

   kde:

   - *soubor_do uší* je `com.ibm.wmqfte.databaselogger.jee.oracle.ear` nebo `com.ibm.wmqfte.databaselogger.jee.ear` v závislosti na tom, zda používáte databázi Db2 nebo Oracle.
   - *soubor_jpa_file* je `com.ibm.wmqfte.web.jpa.oracle.jar` nebo `com.ibm.wmqfte.web.jpa.jar` v závislosti na tom, zda používáte databázi Db2 nebo Oracle.

Jak pokračovat dále

Pomocí upraveného souboru EAR nainstalujte modul pro protokolování databáze Java EE .

Související úlohy

“Instalace modulu protokolování databáze Java EE pro MFT pomocí WebSphere Application Server traditional 9.0” na stránce 774

Při instalaci a konfiguraci modulu pro protokolování databáze Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s operačním systému WebSphere Application Server traditional 9.0postupujte podle těchto pokynů.

Nastavení cesty k nativní knihovně v adresáři WebSphere Application Server traditional 9.0

Pokud implementujete aplikaci modulu pro protokolování databáze Java Platform, Enterprise Edition (Java EE) v systému WebSphere Application Server traditional 9.0a chcete použít připojení v režimu vazeb mezi aplikací a produktem IBM MQ, musíte nakonfigurovat poskytovatele systému zpráv IBM MQ na umístění nativních knihoven IBM MQ v systému.

Informace o této úloze

Pokud nenastavíte cestu k nativní knihovně na aplikačním serveru, můžete obdržet následující chybovou zprávu v systémovém protokolu WebSphere Application Server traditional 9.0 :

```
A connection could not be made to WebSphere MQ for the following reason:
  CC=2;RC=2495;AMQ8568: The native JNI library 'mqjbnd' was not found. [3=mqjbnd]
```

Pomocí administrativní konzoly WebSphere Application Server traditional 9.0 proveďte následující kroky:

Postup

1. V navigačním podokně rozbalte položku **Prostředky** > **JMS** > **Poskytovatelé JMS**.
2. Vyberte poskytovatele systému zpráv IBM MQ , který je ve správném oboru pro továrnu připojení nebo specifikaci aktivace, jež vytváří připojení v režimu vazeb.

   Poznámka: Informace o nativní cestě v rozsahu `Server` se používají jako předvolba k informacím o nativní cestě ve vyšších rozsazích a informace o nativní cestě v rozsahu `Node` se používají jako předvolba k informacím o nativní cestě v rozsahu `Cell` .
3. V části Obecné vlastnosti do pole **Cesta k nativní knihovně** zadejte úplný název adresáře, který obsahuje nativní knihovny IBM MQ .

   Například na Linux zadejte `/opt/mqm/java/lib`. Zadejte pouze jeden název adresáře.
4. Klepněte na tlačítko **OK**.

   Jakmile je cesta nastavena, měli byste uložit změny do hlavní konfigurace, aby se změny projevily.
5. Restartujte aplikační server, abyste obnovili konfiguraci.
6. Požadované: Znovu spusťte aplikační server podruhé, abyste načetli knihovny.

Související úlohy

“Instalace modulu protokolování databáze Java EE pro MFT pomocí WebSphere Application Server traditional 9.0” na stránce 774

Při instalaci a konfiguraci modulu pro protokolování databáze Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s operačním systému WebSphere Application Server traditional 9.0postupujte podle těchto pokynů.

Instalace modulu protokolování databáze Java EE pro MFT pomocí WebSphere Application Server traditional 9.0

Při instalaci a konfiguraci modulu pro protokolování databáze Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s operačním systému WebSphere Application Server traditional 9.0postupujte podle těchto pokynů.

Než začnete

Před instalací aplikace modulu protokolování databáze JEE postupujte podle pokynů v tématech “Příprava na instalaci modulu protokolování databáze Java EE pro MFT” na stránce 772 a “Nastavení cesty k nativní knihovně v adresáři WebSphere Application Server traditional 9.0” na stránce 774.

Informace o této úloze

Další informace o modulu protokolování databáze Java EE naleznete v části “Konfigurace modulu protokolování MFT” na stránce 757.

Postup

1. Nastavte poskytovatele XA JDBC :
   a) V navigaci administrativní konzoly WebSphere Application Server traditional 9.0 vyberte volbu **Prostředky** > **JDBC** > **JDBC** .
   b) Vytvořte poskytovatele JDBC pomocí průvodce konzolou klepnutím na volbu **Nový**.
   c) V kroku 1 průvodce vyberte databázi, kterou používáte, ze seznamu **Typ databáze** a typ přidruženého poskytovatele ze seznamu **Typ poskytovatele** . Ze seznamu **Typ implementace** vyberte volbu **Zdroj dat XA**. Klepněte na tlačítko **Další**.

      z/OS Můžete odebrat odkaz na soubor `db2jcc_license_cisuz.jar` a měli byste změnit `db2jcc.jar` na `db2jcc4.jar`, tj. verzi souboru JAR dodávanou s nejnovější verzí produktu Db2, nebo lokální verzi.
   d) V kroku 2 průvodce se ujistěte, že umístění adresáře požadovaných souborů JAR databáze je správně nastaveno. Klepněte na tlačítko **Další**.
   e) Klepnutím na tlačítko **Dokončit** na souhrnné stránce vytvořte poskytovatele JDBC .
2. Vytvořte aliasy ověřování. Vytvoříte jeden alias pro zdroj dat a druhý pro IBM MQ:
   a) V navigaci konzoly pro správu produktu WebSphere Application Server traditional 9.0 vyberte volbu **Zabezpečení** > **Globální zabezpečení** .
   b) Pod záhlavím **Ověřování** rozbalte položku **Ověřovací a autorizační služba Java**.
   c) Klepněte na volbu **J2C**. Otevře se stránka aliasu ověřování.
   d) Vytvořte alias ověřování pro zdroj dat:
      i) Klepněte na volbu **Nový**.
      ii) Zadejte podrobnosti pro **Alias**, **ID uživatele**, **Heslo**a **Popis**. Podrobnosti zadané v polích **ID uživatele** a **Heslo** se musí shodovat s podrobnostmi, které jste zadali při vytváření uživatele databáze. Další informace viz “Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro MFT” na stránce 779.
      iii) Klepněte na tlačítko **OK**.
   e) Vytvořte alias ověřování pro IBM MQ:
      i) Klepněte na volbu **Nový**.
      ii) Zadejte podrobnosti pro **Alias**, **ID uživatele**, **Heslo**a **Popis**. Podrobnosti zadané v polích **ID uživatele** a **Heslo** se musí shodovat s nastavením uživatele a hesla pro vaši instalaci produktu IBM MQ .
      iii) Klepněte na tlačítko **OK**.
3. Vytvořte zdroj dat:
   a) V navigaci konzoly administrace WebSphere Application Server traditional 9.0 vyberte volbu **Prostředky** > **JDBC** > **Zdroje dat** .
   b) Vyberte rozevírací seznam **Rozsah** a změňte rozsah na příslušnou hodnotu. Například `Node=yourNode, Server=yourServer`.
   c) Vytvořte zdroj dat pomocí průvodce konzolou klepnutím na volbu **Nový**.

d) V kroku 1 průvodce zadejte do pole **Název zdroje dat** hodnotu `wmqfte-database` a do pole **Název rozhraní JNDI** zadejte hodnotu `jdbc/wmqfte-database`. Klepněte na tlačítko **Další**.

e) V kroku 2 průvodce pomocí rozevíracího seznamu **Vybrat existujícího poskytovatele JDBC** vyberte poskytovatele JDBC vytvořeného v předchozích krocích. Klepněte na tlačítko **Další**.

f) **Db2:** V kroku 3 průvodce zadejte do pole **Typ ovladače** hodnotu 4.

g) **Db2:** Zadejte podrobnosti do polí **Název databáze**, **Název serveru**a **Číslo portu** a klepněte na tlačítko **Další**.

Oracle: Zadejte URL připojení do pole **URL** a vyberte správného pomocníka datového úložiště v poli **Název pomocné třídy datového úložiště** .

Oracle RAC: Při připojování ke klastru Oracle Real Application Cluster musí adresa URL URL obsahovat informace o hostiteli nezbytné pro připojení ke všem dostupným instancím databáze.

h) V kroku 4 průvodce vyberte název aliasu ověřování zdroje dat, který jste definovali v kroku 2d ze seznamu **Alias ověřování pro obnovu XA** . Vyberte stejný název ze seznamů **Alias ověřování spravovaný komponentou** a **Alias ověřování spravovaný kontejnerem** .

i) Klepnutím na tlačítko **Dokončit** na souhrnné stránce vytvořte zdroj dat.

4. Volitelné: Ověřte konfiguraci zdroje dat:

a) V navigaci konzoly administrace WebSphere Application Server traditional 9.0 vyberte volbu **Prostředky** > **JDBC** > **Zdroje dat** .

b) Klepněte na tlačítko **Testovat připojení** .

5. Vytvořte téma.

a) V navigaci administrativní konzoly produktu WebSphere Application Server traditional 9.0 klepněte na volbu **Prostředky** > **JMS** > **Témata**.

b) Vyberte rozevírací seznam **Rozsah** a změňte rozsah na příslušnou hodnotu. Například `Node=yourNode, Server=yourServer`.

c) Klepněte na volbu **Nový**.

d) Klepněte na volbu **IBM MQ**.

e) Na panelu **Administrace** stránky vlastností pro dané téma vyberte jedinečné hodnoty pro pole **Název** a **Název rozhraní JNDI** , na které budete později odkazovat v konfiguraci.

f) Na panelu **IBM MQ téma** zadejte do pole **Název tématu** hodnotu `SYSTEM.FTE/Log/#` .

6. Vytvořte specifikaci aktivace:

a) V navigaci administrativní konzoly produktu WebSphere Application Server traditional 9.0 klepněte na volbu **Prostředky** > **JMS** > **Specifikace aktivace**.

b) Vyberte rozevírací seznam **Rozsah** a změňte rozsah na příslušnou hodnotu. Například `Node=yourNode, Server=yourServer`.

c) Klepněte na volbu **Nový**.

d) Klepněte na volbu **IBM MQ**.

e) V kroku 1 průvodce zvolte jedinečné hodnoty pro pole **Název** a **Název rozhraní JNDI** , na které budete později v konfiguraci znovu odkazovat.

f) V kroku 1.1zadejte název rozhraní JNDI pro téma, které jste nastavili v kroku 5, do pole **Název cílového rozhraní JNDI** .

g) V seznamu **Typ cíle** vyberte volbu **Téma**.

h) V kroku 1.2 průvodce vyberte volbu **Trvalý odběr**. Zadejte `SYSTEM.FTE.DATABASELOGGER.AUTO` do pole **Název odběru** .

i) V kroku 2 průvodce vyberte volbu **Zadat všechny požadované informace do tohoto průvodce**.

j) V kroku 2.1zadejte název správce front do pole **Název správce front nebo skupiny sdílení front** .

k) V kroku 2.2vyberte vybranou metodu přenosu ze seznamu **Přenos** . Vyberete-li volbu **Vazby**, nejsou vyžadovány žádné další informace. Pokud vyberete volbu **Klient** nebo **Vazby, pak klient**, zadejte podrobnosti pro **Název hostitele**, **Port**a **Kanál připojení serveru**.

l) Volitelné: Klepnutím na tlačítko **Testovat připojení** potvrďte, že je přítomen správce front. Můžete však očekávat, že přijmete `NOT_AUTHORIZED` , dokud neodkazujete na alias ověřování v kroku 6n.

m) Klepněte na tlačítko **Uložit**.

n) Klepněte na název specifikace aktivace, kterou jste vytvořili. V sekci **Obecné vlastnosti** na kartě **Konfigurace** se posuňte dolů na panel **Rozšířené** a zadejte jedinečný název pro identifikaci připojení IBM MQ do pole **ID klienta** . Musíte dokončit tento krok, jinak bude vaše připojení odmítnuto produktem IBM MQ s kódem chyby `JMSCC0101` .

o) Pokud jste jako metodu přenosu vybrali volbu **Klient** , přejděte na panel **Nastavení zabezpečení** a vyberte alias ověřování, který jste definovali v kroku 8, ze seznamu **Alias ověřování** .

p) Klepněte na tlačítko **Použít**.

q) V sekci **Další vlastnosti** na kartě **Konfigurace** klepněte na volbu **Rozšířené vlastnosti**. V sekci **Konzument připojení** panelu **Rozšířené vlastnosti** zadejte do pole **Maximální počet relací serveru** hodnotu `1` .

Poznámka: Než budete pokračovat, ujistěte se, že jste dokončili tento krok. Pokud tak neučinění neučiní, může dojít k selhání modulu protokolování.

r) V sekci **Další vlastnosti** na kartě **Konfigurace** klepněte na volbu **Rozšířené vlastnosti**. Nastavte hodnotu **Zastavit koncový bod, pokud se doručení zprávy nezdaří** na minimum `1`.

Je-li hodnota vlastnosti **`_numberOfFailedAttemptsBeforeReject`** nastavena na více než 1 (další informace viz 9j), nastavte volbu **Zastavit koncový bod, pokud se doručení zprávy nezdaří** alespoň na hodnotu vlastnosti **`_numberOfFailedAttemptsBeforeReject`** . To zabrání zastavení koncového bodu, když je přijata zpráva, kterou nelze zpracovat (například chybná zpráva protokolu přenosu). Další informace viz MFT ošetření chyb a odmítnutí modulu protokolování.

7. Vytvořte továrnu připojení fronty.

a) V navigaci administrativní konzoly produktu WebSphere Application Server traditional 9.0 klepněte na volbu **Prostředky** > **JMS** > **Továrny připojení fronty**.

b) Vyberte rozevírací seznam **Rozsah** a změňte rozsah na příslušnou hodnotu. Například `Node=yourNode, Server=yourServer`.

c) Klepněte na volbu **Nový**.

d) Klepněte na volbu **IBM MQ**.

e) V kroku 1 průvodce zvolte jedinečné hodnoty pro pole **Název** a **Název rozhraní JNDI** , na které budete později v konfiguraci znovu odkazovat.

f) V kroku 2 vyberte volbu **Zadat všechny požadované informace do tohoto průvodce**.

g) V kroku 2.1zadejte název správce front do pole **Název správce front nebo skupiny sdílení front** .

h) V kroku 2.2vyberte vybranou metodu přenosu ze seznamu **Přenos** . Vyberete-li volbu **Vazby**, nejsou vyžadovány žádné další informace. Pokud vyberete volbu **Klient** nebo **Vazby, pak klient**, zadejte podrobnosti pro **Název hostitele**, **Port**a **Kanál připojení serveru**.

i) Volitelné: Klepnutím na tlačítko **Testovat připojení** potvrďte, že je přítomen správce front. Můžete však očekávat, že přijmete `NOT_AUTHORIZED` , dokud neodkazujete na alias ověřování v kroku 7h.

j) Pokud jste jako metodu přenosu vybrali volbu **Klient** nebo **Vazby poté klient** , klepněte na název továrny připojení fronty, kterou jste právě vytvořili. Posuňte se dolů na panel **Nastavení zabezpečení** na kartě **Konfigurace** a vyberte alias ověřování, který jste definovali v kroku 2e , ze seznamů **Alias ověřování pro zotavení XA** a **Alias ověřování spravovaný kontejnerem** .

8. Vytvořte frontu odmítnutí v adresáři WebSphere Application Server:

a) V navigaci administrativní konzoly produktu WebSphere Application Server traditional 9.0 klepněte na volbu **Prostředky** > **JMS** > **Fronty**.

b) Vyberte rozevírací seznam **Rozsah** a změňte rozsah na příslušnou hodnotu. Například `Node=yourNode, Server=yourServer`.

c) Klepněte na volbu **Nový**.

d) Klepněte na volbu **IBM MQ**.

e) Vyberte jedinečné hodnoty pro pole **Název** a **Název rozhraní JNDI** , na které budete později v konfiguraci znovu odkazovat.

f) Do pole **Název fronty** zadejte hodnotu SYSTEM.FTE.LOG.RJCT.*logger_name* . Ujistěte se, že jste tuto frontu vytvořili v koordinačním správci front.

g) Do pole **Název správce front** zadejte název správce front.

h) Klepněte na tlačítko **OK**.

9. Nainstalujte aplikaci modulu protokolování databáze JEE:

a) V konzole pro správu produktu WebSphere Application Server traditional 9.0 vyberte volbu **Aplikace** > **Nová aplikace**.

b) Vyberte rozevírací seznam **Rozsah** a změňte rozsah na příslušnou hodnotu. Například `Node=yourNode, Server=yourServer`.

c) Ze seznamu voleb vyberte volbu **Nová podniková aplikace**.

d) Na stránce **Příprava na instalaci aplikace** vyberte soubor `com.ibm.wmqfte.databaselogger.jee.ear` nebo soubor `com.ibm.wmqfte.databaselogger.jee.oracle.ear` z adresáře *MQ_INSTALLATION_PATH*`/mqft/web` instalace Managed File Transfer Service a klepněte na tlačítko **Další**.

e) Na následující obrazovce vyberte volbu **Podrobná** , abyste zobrazili všechny volby a parametry instalace, a klepněte na tlačítko **Další**.

f) Klepnutím na tlačítko **Další** v průvodci kroky 1-4 přijmete výchozí hodnoty.

g) V kroku 5 průvodce **Svázat listenery pro objekty typu message-driven bean**se posuňte do části **Vazby modulu listener** . Klepněte na volbu **Specifikace aktivace**.

Zadejte požadované hodnoty pro následující pole:

Název rozhraní JNDI cílového prostředku
Název rozhraní JNDI, který jste zadali při vytváření specifikace aktivace v kroku 6d.

Název cílového rozhraní JNDI
Název rozhraní JNDI, který jste zadali při vytváření tématu v kroku 5d.

Klepněte na tlačítko **Další**.

h) V kroku 6 průvodce **Mapovat odkazy na prostředky na prostředky**zadejte podrobnosti do pole **Název rozhraní JNDI cílového prostředku** . Tento název je název rozhraní JNDI, který jste zadali pro továrnu připojení fronty odmítnutí v kroku 7c. Klepněte na tlačítko **Další**.

i) V kroku 7 průvodce **Mapovat odkazy na položky prostředí prostředků na prostředky**zadejte podrobnosti do pole **Název rozhraní JNDI cílového prostředku** . Tento název je název rozhraní JNDI fronty odmítnutí, kterou jste vytvořili v kroku 8d. Klepněte na tlačítko **Další**.

j) V kroku 8 průvodce **Mapovat položky prostředí pro moduly EJB**přijměte výchozí hodnotu 1. Klepněte na tlačítko **Další**.

Oracle RAC: Při připojování ke klastru Oracle Real Application Cluster musíte nastavit hodnotu vlastnosti _numberOfFailedAttemptsBeforeReject na **alespoň** 2. Tato vlastnost určuje počet pokusů modulu protokolování o zpracování zprávy auditu po výskytu selhání. V případě překonání selhání databáze se pravděpodobně vyskytne alespoň jedno selhání. Chcete-li se vyhnout zbytečnému přesunu zprávy do fronty odmítnutí, zvýšení této hodnoty umožní provést druhý pokus, což obvykle vede k úspěchu při vytváření připojení k nové instanci databáze. Pokud během testování zjistíte, že zprávy jsou stále přesunuty do fronty odmítnutí během překonání selhání instance databáze, zvyšte tuto hodnotu dále: časování přepínače mezi instancemi může způsobit více než jedno selhání pro stejnou zprávu. Mějte však na paměti, že zvýšení této hodnoty ovlivní všechny případy selhání (například chybnou zprávu) a nikoli pouze překonání selhání databáze, proto zvyšte hodnotu opatrně, abyste se vyhnuli zbytečným opakovaným pokusům.

k) V kroku 9 průvodce **Metadata pro moduly**klepněte na tlačítko **Další**.

l) V kroku 10 průvodce **Souhrn**klepněte na tlačítko **Dokončit**.

10. Nyní můžete spustit aplikaci z konzoly pro správu WebSphere Application Server traditional 9.0 :
    a) V navigaci konzoly vyberte volbu **Aplikace** > **Typy aplikací** > **WebSphere** .
    b) Označte zaškrtávací políčko pro podnikovou aplikaci **Logger** z tabulky kolekce a klepněte na tlačítko **Spustit**.

Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro MFT

Při konfiguraci modulu protokolování databáze Java Platform, Enterprise Edition (Java EE) pro systém Managed File Transferpotřebujete uživatelské účty pro přístup k produktu IBM MQ, k databázi a k operačnímu systému. Počet požadovaných uživatelů operačního systému závisí na počtu systémů, které používáte k hostování těchto komponent.

Informace o této úloze

Počet a typ uživatelských účtů, které potřebujete ke spuštění modulu protokolování databáze Java EE , závisí na počtu používaných systémů. Uživatelské účty jsou nezbytné pro přístup k následujícím třem prostředím:

- Lokální operační systém
- IBM MQ
- Databáze

Modul pro protokolování databáze JEE, IBM MQ a vaši databázi můžete nainstalovat na jeden systém nebo na více systémů. Komponenty lze instalovat v následujících vzorových topologiích:

Java EE modul pro protokolování databáze IBM MQa databáze ve stejném systému.
Můžete definovat jednoho uživatele operačního systému pro použití se všemi třemi komponentami. Modul protokolování používá režim vazeb pro připojení k produktu IBM MQ a nativní připojení pro připojení k databázi.

Java EE modul pro protokolování databáze a IBM MQ v jednom systému, databáze v odděleném systému.
Pro tuto konfiguraci vytvoříte dva uživatele: uživatele operačního systému na systému, na kterém je spuštěn modul protokolování, a uživatele operačního systému se vzdáleným přístupem k databázi na databázovém serveru. Modul protokolování používá režim vazeb pro připojení k produktu IBM MQ a připojení klienta pro přístup k databázi.

Java EE modul pro protokolování databáze v jednom systému, IBM MQ v jiném systému, databáze v dalším systému.
Pro tuto konfiguraci vytvoříte tři uživatele: uživatele operačního systému pro spuštění aplikačního serveru, uživatele systému IBM MQ pro přístup k používaným frontám a tématům a uživatele databázového serveru pro přístup a vkládání do databázových tabulek. Modul protokolování používá režim klienta pro přístup k produktu IBM MQ a připojení klienta pro přístup k databázi.

Jako příklad zbytek těchto pokynů předpokládá, že se uživatel nazývá `ftelog`, ale můžete použít libovolné jméno uživatele, nové nebo existující. Nakonfigurujte oprávnění uživatele takto:

Postup

1. Ujistěte se, že uživatel operačního systému má svou vlastní skupinu a není také ve skupinách s rozsáhlými oprávněními pro koordinačního správce front. Uživatel by neměl být ve skupině mqm. Na určitých platformách je skupině personálu také automaticky udělen přístup ke správci front; uživatel modulu protokolování by neměl být ve skupině personálu. Pomocí konzoly IBM MQ Explorermůžete zobrazit záznamy oprávnění pro samotného správce front a pro objekty v něm obsažené. Klepněte pravým tlačítkem myši na objekt a vyberte volbu **Oprávnění k objektu > Spravovat záznamy oprávnění**. Na příkazovém řádku můžete použít příkazy dspmqaut (oprávnění k zobrazení) nebo dmpmqaut (oprávnění k výpisu paměti).
2. Použijte okno **Spravovat záznamy oprávnění** v příkazu IBM MQ Explorer nebo setmqaut (udělit nebo odvolat oprávnění) k přidání oprávnění pro vlastní skupinu uživatele IBM MQ (na systému AIXjsou

oprávnění IBM MQ přidružena pouze ke skupinám, ne jednotlivým uživatelům). Požadované orgány jsou tyto:

- CONNECT a INQUIRE ve správci front (ke zpracování v knihovnách produktu IBM MQ Java je vyžadováno oprávnění INQUIRE).
- Oprávnění ODEBÍRAT v systému SYSTEM.FTE .
- Oprávnění PUT v systému SYSTEM.FTE.LOG.RJCT. Fronta*logger_name* .

Zadané názvy front odmítnutí a příkazů jsou předvolené názvy. Pokud jste při konfiguraci front modulu protokolování zvolili různé názvy front, přidejte oprávnění k těmto názvům front.

3. Proveďte konfiguraci uživatele databáze, která je specifická pro databázi, kterou používáte.
   - Pokud je vaše databáze Db2, postupujte takto:

     Poznámka: Existuje několik mechanizmů pro správu uživatelů databáze s produktem Db2. Tyto pokyny se vztahují na výchozí schéma založené na uživatelích operačního systému.

     – Ujistěte se, že uživatel `ftelog` není v žádné skupině administrace Db2 (například db2iadm1, db2fadm1nebo dasadm1).

     – Udělte uživateli oprávnění pro připojení k databázi a oprávnění k výběru, vložení a aktualizaci tabulek, které jste vytvořili v rámci kroku 2: vytvoření požadovaných databázových tabulek.
   - Pokud je vaše databáze Oracle, postupujte takto:

     – Ujistěte se, že uživatel `ftelog` není v žádné skupině administrace Oracle (například ora_dba na systému Windows nebo dba na systému AIX and Linux).

     – Udělte uživateli oprávnění k připojení k databázi a oprávnění k výběru, vložení a aktualizaci tabulek, které jste vytvořili v rámci kroku 2: vytvoření požadovaných databázových tabulek.

Migrace ze samostatného modulu pro protokolování databáze na modul pro protokolování databáze Java EE pro MFT

Můžete provést migraci ze samostatného modulu pro protokolování databáze do modulu pro protokolování databáze Java EE . Musíte zastavit samostatný modul pro protokolování databáze a nainstalovat modul pro protokolování databáze JEE. Chcete-li zabránit ztrátě nebo duplikaci položek protokolu, musíte před zastavením samostatného modulu pro protokolování databáze zastavit publikování zpráv v tématu SYSTEM.FTE a po instalaci modulu pro protokolování databáze Java EE jej znovu spustit. Před migrací zálohujte databázi.

Informace o této úloze

Postup

1. Před zastavením databáze spusťte pro koordinačního správce front následující příkaz MQSC: `ALTER QM PSMODE(COMPAT)`

   Tím se zastaví publikování zpráv do SYSTEM.FTE/Log . Počkejte, až modul protokolování zpracuje všechny zprávy na svém odběru. Standardně se tento odběr nazývá SYSTEM.FTE.LOGGER.AUTO.
2. Zastavte modul pro protokolování databáze pomocí příkazu **`fteStopLogger`** .
3. Zálohujte databázi pomocí nástrojů dodaných s databázovým softwarem.
4. Odstraňte odběr, který patří do samostatného modulu pro protokolování databáze.

   Standardně se tento odběr nazývá SYSTEM.FTE.LOGGER.AUTO.
5. Pokud je vaše schéma databáze na dřívější verzi, musíte migrovat schéma na každou následující úroveň v pořadí. Například, pokud je vaše schéma databáze na V7.0.1 a provádíte migraci na V7.0.4, musíte migrovat své schéma z V7.0.1 na V7.0.2, pak z V7.0.2 na V7.0.3a pak z V7.0.3 na V7.0.4. Migrujte schéma databáze z verze *`old`* na verzi *new*, kde *`old`* a *new* jsou proměnné, které popisují verzi schématu, provedením jedné z následujících akcí pro každou verzi schématu, kterou musíte migrovat:

- z/OS Pokud je vaše databáze Db2 na systému z/OS a provádíte migraci mezi schématy V7.0.2 a V7.0.3 nebo mezi schématy V7.0.3 a V7.0.4 , musíte vytvořit nové schéma databáze a zkopírovat do něj existující data. Další informace naleznete v dokumentaci agenta Db2.
- Pokud vaše databáze není Db2 nebo pokud jste vytvořili databázi s velikostí stránky větší než 8K, můžete migrovat schéma stejným způsobem jako pro ostatní verze provedením následujících kroků.
- Provádíte-li migraci mezi databázovými tabulkami za jiných okolností, postupujte takto:
  a. Vyberte soubor, který odpovídá vaší databázové platformě, a který má název obsahující řetězec *old-new*. Tento soubor je umístěn v adresáři *MQ_INSTALLATION_PATH*/mqft/sql instalace vzdálených nástrojů a dokumentace.
  b. Pokud jste provedli úpravy počátečního schématu, zkontrolujte soubor migrace a ujistěte se, že bude kompatibilní s vaší upravenou databází.
  c. Spusťte soubor SQL pro vaši databázi.

6. Nainstalujte soubor EAR modulu pro protokolování databáze Java EE .
7. Implementujte modul pro protokolování databáze Java EE . Další informace viz téma "Instalace modulu protokolování databáze Java EE pro MFT" na stránce 771.
8. Spusťte následující příkaz MQSC pro koordinačního správce front: `ALTER QMGR PSMODE(ENABLED)`
   To umožňuje publikování zpráv do systému SYSTEM.FTE/Log .

Výsledky

Konfigurace mostu Connect:Direct

Nakonfigurujte most Connect:Direct pro přenos souborů mezi sítí Managed File Transfer a sítí Connect:Direct . Komponenty mostu Connect:Direct jsou uzel Connect:Direct a agent Managed File Transfer , který je vyhrazen pro komunikaci s tímto uzlem. Na tohoto agenta se odkazuje jako na agenta mostu Connect:Direct .

Než začnete

Agent a uzel, který tvoří most Connect:Direct, musí být na stejném systému nebo mít přístup ke stejnému systému souborů, například prostřednictvím sdíleného připojení NFS. Tento systém souborů se používá k dočasnému ukládání souborů během přenosů souborů, které zahrnují most Connect:Direct, do adresáře definovaného v parametru **cdTmpDir**. Agent mostu Connect:Direct a uzel mostu Connect:Direct musí mít možnost adresovat tento adresář pomocí stejného názvu cesty. Pokud se například agent a uzel nachází v samostatných systémech Windows, musí systémy používat stejné písmeno jednotky k připojení sdíleného systému souborů. Následující konfigurace umožňují agentovi a uzlu používat stejný název cesty:

- Agent a uzel jsou na stejném systému, který běží buď v Windows, nebo Linux for x86-64.
- Agent je v systému Linux for x86-64 a uzel je v systému AIX.
- Agent je v jednom systému Windows a uzel se nachází na jiném systému Windows .

Následující konfigurace neumožňují agentovi a uzlu použít stejný název cesty:

- Agent je v systému Linux for x86-64 a uzel je v systému Windows.
- Agent je v systému Windows a uzel je v systému UNIX.

Zvažte toto omezení při plánování instalace mostu Connect:Direct.

Další podrobnosti o verzích operačního systému podporovaných pro most Connect:Direct naleznete na webové stránce Systémové požadavky pro produkt IBM MQ.

Informace o této úloze

Agent mostu Connect:Direct je agent Managed File Transfer , který je vyhrazen pro komunikaci s uzlem Connect:Direct .

Standardně agent mostu Connect:Direct používá protokol TCP/IP pro připojení k uzlu Connect:Direct . Chcete-li zabezpečené připojení mezi agentem mostu Connect:Direct a uzlem Connect:Direct , můžete použít protokol SSL nebo protokol TLS.

Postup

1. Zvolte operační systémy pro agenta a uzel mostu Connect:Direct :
   a) Vyberte systém, na kterém běží Windows nebo Linux na x86-64 , na kterém se má nainstalovat agent mostu Connect:Direct .
   b) Vyberte operační systém, který je podporován produktem Connect:Direct for Windows nebo Connect:Direct for UNIX pro instalaci uzlu mostu Connect:Direct .
2. Zvolte a nakonfigurujte uzel Connect:Direct .

   Před provedením těchto pokynů musíte mít nainstalovaný uzel Connect:Direct .
   a) Vyberte uzel Connect:Direct , se kterým má agent Managed File Transfer komunikovat.
   b) Zkontrolujte mapu sítě pro zvolený uzel Connect:Direct . Pokud mapa sítě obsahuje položky pro vzdálené uzly spuštěné v operačním systému Windows , musíte zajistit, aby tyto položky uváděly, že jsou uzly spuštěny v systému Windows.

      Pokud je uzel Connect:Direct , který jste vybrali pro most Connect:Direct , spuštěn v systému Windows, upravte síťovou mapu pomocí volby Connect:Direct Žadatel. Ujistěte se, že pole **Operační systém** pro všechny vzdálené uzly spuštěné v systému Windows je nastaveno na **Windows**.
3. Vytvořte a nakonfigurujte agenta mostu Connect:Direct .
   a) Vytvořte agenta mostu Connect:Direct pomocí příkazu **fteCreateCDAgent** .
      - Musíte zadat hodnotu pro parametr **cdNode** . Tento parametr určuje název, který agent používá pro uzel Connect:Direct , který je součástí mostu Connect:Direct . Použijte název uzlu Connect:Direct , který jste vybrali v předchozí sekci.
      - Zadejte hodnoty pro parametry **cdNodeHost** a **cdNodePort** , které definují uzel Connect:Direct , se kterým agent komunikuje.

        Pokud nezadáte hodnotu pro parametr **cdNodeHost** , použije se název hostitele nebo adresa IP lokálního systému. Pokud nezadáte hodnotu pro parametr **cdNodePort** , použije se hodnota 1363 .
      - Volitelně použijte informace v fteCreateAgent k určení, zda potřebujete uvést hodnotu pro parametr **cdTmpDir** .
   b) Namapujte pověření uživatele používaná produktem Managed File Transfer na pověření uživatele na uzlu Connect:Direct . Pověření můžete mapovat pomocí jedné z následujících metod:
      - Vytvořte soubor `ConnectDirectCredentials.xml` pro definování informací o mapování pověření. Další informace viz téma “Mapování pověření pro produkt Connect:Direct pomocí souboru ConnectDirectCredentials.xml” na stránce 783.
      - Zapište uživatelskou proceduru pro provedení mapování pověření pro most Connect:Direct . Další informace viz téma “Mapování pověření pro produkt Connect:Direct pomocí tříd ukončení” na stránce 786.
4. Nakonfigurujte soubor `ConnectDirectNodeProperties.xml` tak, aby obsahoval informace o vzdálených uzlech Connect:Direct .

   Před provedením těchto pokynů musíte vytvořit agenta mostu Connect:Direct .

   Upravte šablonu `ConnectDirectNodeProperties.xml` v konfiguračním adresáři agenta mostu Connect:Direct . Pro každý uzel Connect:Direct nebo skupinu uzlů, o kterých chcete definovat informace, postupujte takto:

   a) Uvnitř prvku nodeProperties vytvořte prvek node .

b) Přidejte atribut name do prvku node . Uveďte hodnotu tohoto atributu jako vzor, aby se shodovala s názvem jednoho nebo více vzdálených uzlů Connect:Direct .

c) Volitelné: Přidejte atribut pattern do prvku node , který uvádí, jaký typ vzoru má hodnota v atributu name . Platné hodnoty jsou `regex` a `wildcard`. Výchozí volba je `wildcard`.

d) Přidejte atribut type do prvku node , který uvádí operační systém, na kterém běží vzdálené uzly Connect:Direct uvedené atributem name .

Platné jsou tyto hodnoty:

- `Windows` -Uzel běží na Windows
- `UNIX` -uzel je spuštěn na AIX and Linux
- z/OS `z/OS`, `zos`, `os/390`nebo `os390` -Uzel běží na z/OS

Hodnota tohoto atributu nerozlišuje velikost písmen. Přenosy do vzdálených uzlů v jiných operačních systémech most Connect:Direct nepodporuje.

Další informace viz Connect:Direct formát souboru vlastností uzlu.

5. Nakonfigurujte zabezpečené připojení mezi agentem mostu Connect:Direct a uzlem Connect:Direct . Příklad, jak to provést, viz téma Konfigurace SSL nebo TLS mezi agentem mostu Connect:Direct a uzlem Connect:Direct.

Související úlohy

Odstraňování problémů s mostem Connect:Direct

Konfigurace zabezpečení SSL nebo TLS mezi agentem mostu Connect:Direct a uzlem Connect:Direct

Přenos souboru do uzlu Connect:Direct

Přenos souboru z uzlu Connect:Direct

z/OS Přenos více souborů z uzlu Connect:Direct

Související odkazy

Most Connect:Direct

Pověření mapování pro Connect:Direct

Namapujte pověření uživatele v produktu Managed File Transfer na pověření uživatele na uzlu Connect:Direct pomocí výchozí funkce mapování pověření agenta mostu Connect:Direct nebo napsáním vlastní uživatelské procedury. Produkt Managed File Transfer poskytuje ukázkovou uživatelskou proceduru, která provádí mapování pověření uživatele.

Související úlohy

“Mapování pověření pro produkt Connect:Direct pomocí souboru ConnectDirectCredentials.xml” na stránce 783

Namapujte pověření uživatele v produktu Managed File Transfer na pověření uživatele na uzlech Connect:Direct pomocí výchozí funkce mapování pověření agenta mostu Connect:Direct . Produkt Managed File Transfer poskytuje soubor XML, který můžete upravit tak, aby obsahoval informace o pověření.

“Mapování pověření pro produkt Connect:Direct pomocí tříd ukončení” na stránce 786

Pokud nechcete použít výchozí funkci mapování pověření agenta mostu Connect:Direct , můžete namapovat pověření uživatele v produktu Managed File Transfer na pověření uživatele v uzlu Connect:Direct napsáním vlastní uživatelské procedury. Konfigurace vlastních uživatelských procedur mapování pověření zakáže výchozí funkci mapování pověření.

Související odkazy

CDCredentialExitrozhraní .java

Formát souboru pověření Connect:Direct

Mapování pověření pro produkt Connect:Direct pomocí souboru ConnectDirectCredentials.xml

Namapujte pověření uživatele v produktu Managed File Transfer na pověření uživatele na uzlech Connect:Direct pomocí výchozí funkce mapování pověření agenta mostu Connect:Direct . Produkt

Managed File Transfer poskytuje soubor XML, který můžete upravit tak, aby obsahoval informace o pověření.

Informace o této úloze

Po vytvoření agenta mostu Connect:Direct pomocí příkazu **fteCreateCDAgent** je třeba ručně vytvořit soubor `ConnectDirectCredentials.xml` . Než budete moci použít agenta mostu Connect:Direct , musíte upravit tento soubor tak, aby obsahoval informace o hostiteli, uživateli a pověření. Další informace viz Connect:Direct. Standardně se tento soubor načítá z domovského adresáře aktuálního uživatele, například `/home/fteuser/ConnectDirectCredentials.xml` . Chcete-li použít jiné umístění, zadejte jej pomocí prvku `<credentialsFile>` v souboru `ConnectDirectNodeProperties.xml` .

Postup

1. Ujistěte se, že atribut `name` v prvku `<tns:pnode name="Connect:Direct node host" pattern="wildcard">` obsahuje hodnotu názvu uzlu Connect:Direct , ke kterému se připojuje agent mostu Connect:Direct . Tato hodnota musí být stejná jako hodnota, kterou zadáte pro parametr **fteCreateCDAgent -cdNode** .

   Hodnota atributu `pattern` může být buď `wildcard` , nebo `regex`. Není-li tento atribut uveden, předvolba je `wildcard`.
2. Vložte ID uživatele a informace o pověření do souboru jako podřízené prvky prvku `<tns:pnode>`.

   Do souboru můžete vložit jednu nebo více instancí následujícího prvku `<tns:user>` :

   ```
   <tns:user name="name"
             pattern="pattern"
             ignorecase="ignorecase"
             cdUserId="cdUserId"
             cdPassword="cdPassword"
             pnodeUserId="pnodeUserId"
             pnodePassword="pnodePassword">
   </tns:user>
   ```

   kde:

   - *name* je vzor odpovídající ID uživatele MQMD přidruženému k požadavku na přenos MFT .
   - Parametr *pattern* určuje, zda je vzor určený pro atribut `name` výrazem se zástupným znakem nebo Java regulárním výrazem. Hodnota atributu `pattern` může být buď `wildcard` , nebo `regex`. Není-li tento atribut uveden, předvolba je `wildcard`.
   - Parametr *ignorecase* určuje, zda má být se vzorem určeným atributem `name` zacházeno s rozlišením velkých a malých písmen. Není-li tento atribut uveden, předvolba je `true`.
   - *cdUserId* je ID uživatele, které používá agent mostu Connect:Direct pro připojení k uzlu Connect:Direct určenému atributem `name` prvku `<tns:pnode>` . Je-li to možné, ujistěte se, že *cdUserId* je ID administrátora Connect:Direct . Pokud *cdUserId* nemůže být administrátorem produktu Connect:Direct , ujistěte se, že má ID uživatele následující funkční oprávnění na uzlu mostu Connect:Direct :

     – Pro uzel Windows nastavte následující oprávnění. Tento příklad je formátován s návratem vozíku pro lepší čitelnost:

     ```
     View Processes in the  value: yes
      TCQ
     Issue the copy         value: yes
      receive, copy send,
      run job, and run task
      Process statements
     Issue the submit       value: yes
      Process statement
     Monitor, submit,       value: all
      change,and delete all
      Processes
     Access Process         value: all
     ```

```
 statistics
Use the trace tool or  value: yes
 issue traceon and
 traceoff commands
Override Process       value: yes
 options such as file
 attributes and remote
 node ID
```

– Pro uzel AIX nebo Linux nastavte v souboru `userfile.cfg` následující parametry:

```
pstmt.copy             value: y
pstmt.upload           value: y
pstmt.download         value: y
pstmt.runjob           value: y
pstmt.runtask          value: y
cmd.submit             value: y
pstmt.submit           value: y
cmd.chgproc            value: y
cmd.delproc            value: y
cmd.flsproc            value: y
cmd.selproc            value: a
cmd.selstats           value: a
cmd.trace              value: y
snode.ovrd             value: y
```

- *cdPassword* je heslo přidružené k ID uživatele uvedenému v atributu `cdUserId` .
- Volitelně můžete uvést atribut `pnodeUserId` . Hodnota tohoto atributu je ID uživatele, které používá uzel Connect:Direct určený atributem `name` prvku `<tns:pnode>` k odeslání procesu Connect:Direct . Pokud neuvedete atribut `pnodeUserId` , uzel Connect:Direct použije ID uživatele uvedené atributem `cdUserId` k odeslání procesu Connect:Direct .
- Volitelně můžete uvést atribut `pnodePassword`. Hodnota tohoto atributu je heslo přidružené k ID uživatele uvedenému atributem `pnodeUserId` .

Pokud se ID uživatele MQMD neshoduje s žádným prvkem uživatele, přenos se nezdaří.

3. Volitelné: Jako podřízené prvky prvku `<tns:user>` můžete zahrnout jeden nebo více prvků `<tns:snode>` . Prvek `<tns:snode>` určuje pověření používaná uzlem Connect:Direct , který je součástí mostu Connect:Direct . Tato pověření jsou ID uživatele a heslo, které uzel mostu Connect:Direct používá pro připojení k uzlu Connect:Direct , který je zdrojem nebo cílem přenosu souborů.

   Vložte do souboru jeden nebo více následujících prvků:

```
<tns:snode name="name"
           pattern="pattern"
           userId="userId"
           password="password"/>
```

   kde:

   - *name* je vzor odpovídající názvu uzlu Connect:Direct , který je zdrojem nebo cílem přenosu souborů.
   - Parametr *pattern* určuje, zda je vzor určený pro atribut `name` výrazem se zástupným znakem nebo Java regulárním výrazem. Hodnota atributu vzorku může být buď `wildcard` , nebo `regex`. Není-li tento atribut uveden, předvolba je `wildcard`.
   - *userId* je ID uživatele, které používá uzel Connect:Direct určený atributem `name` prvku `<tns:pnode>` pro připojení k uzlu Connect:Direct , který odpovídá vzoru určenému atributem `name` `<tns:snode>`.
   - *password* je heslo přidružené k ID uživatele uvedenému v atributu `userId` .

   Pokud žádný prvek `<tns:snode>` neodpovídá sekundárnímu uzlu přenosu souborů, nezpůsobí to selhání přenosu. Přenos je spuštěn a není zadáno žádné ID uživatele a heslo pro použití s uzlem snode.

Výsledky

Při hledání shody se vzorem pro jména uživatelů nebo názvy uzlů Connect:Direct agent mostu Connect:Direct vyhledává od začátku souboru do konce souboru. První nalezená shoda je ta, která se použije.

Související úlohy

“Konfigurace mostu Connect:Direct” na stránce 781

Nakonfigurujte most Connect:Direct pro přenos souborů mezi sítí Managed File Transfer a sítí Connect:Direct . Komponenty mostu Connect:Direct jsou uzel Connect:Direct a agent Managed File Transfer , který je vyhrazen pro komunikaci s tímto uzlem. Na tohoto agenta se odkazuje jako na agenta mostu Connect:Direct .

Související odkazy

Formát souboru pověření Connect:Direct

fteCreateCDAgent: vytvořte agenta mostu Connect:Direct .

Mapování pověření pro produkt Connect:Direct pomocí tříd ukončení

Pokud nechcete použít výchozí funkci mapování pověření agenta mostu Connect:Direct , můžete namapovat pověření uživatele v produktu Managed File Transfer na pověření uživatele v uzlu Connect:Direct napsáním vlastní uživatelské procedury. Konfigurace vlastních uživatelských procedur mapování pověření zakáže výchozí funkci mapování pověření.

Informace o této úloze

Uživatelské procedury, které vytvoříte pro mapování Connect:Direct pověření, musí implementovat rozhraní `com.ibm.wmqfte.exitroutine.api.ConnectDirectCredentialExit`. Další informace viz CDCredentialExitrozhraní .java.

Konfigurace IBM MQ Console a REST API

Server mqweb, který je hostitelem IBM MQ Console a REST API , je poskytován s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh, například konfiguraci zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny dostupné volby konfigurace.

Procedura

- “Základní konfigurace pro server mqweb” na stránce 787
- “Konfigurace zabezpečení” na stránce 792
- “Konfigurace názvu hostitele HTTP” na stránce 792
- “Konfigurace portů HTTP a HTTPS” na stránce 793
- “Konfigurace časového limitu odezvy” na stránce 795
- “Konfigurace automatického spuštění” na stránce 795
- “Konfigurace protokolování” na stránce 796
- “Konfigurace tokenu LTPA” na stránce 800
- “Konfigurace chování připojení vzdáleného správce front pro IBM MQ Console” na stránce 802
- “Konfigurace brány administrative REST API” na stránce 804
- “Konfigurace agenta messaging REST API” na stránce 805
- “Konfigurace REST API pro MFT” na stránce 811
- “Vyladění prostředí JVM serveru mqweb” na stránce 816
- “Struktura souboru komponenty instalace IBM MQ Console a REST API” na stránce 818

Základní konfigurace pro server mqweb

Než začnete používat REST API nebo IBM MQ Console, musíte nainstalovat správné komponenty a nakonfigurovat server mqweb, který hostuje REST API nebo IBM MQ Console.

Informace o této úloze

Procedura pro tuto úlohu se zaměřuje na základní konfiguraci serveru mqweb, abyste mohli rychle začít s REST API a IBM MQ Console. Kroky pro konfiguraci osnovy zabezpečení, jak nastavit základní registr uživatelů, ale existují další volby pro konfiguraci uživatelů a rolí. Další informace o konfiguraci zabezpečení pro server mqweb naleznete v části IBM MQ Console a REST API zabezpečení.

Poznámka: Chcete-li provést tento postup, musíte mít přístup k souboru `mqwebuser.xml` :

- z/OS V systému z/OSmusíte být uživatelem, který má přístup pro zápis do souboru `mqwebuser.xml` .
- Multi Na všech ostatních operačních systémech musíte být privilegovaný uživatel pro přístup k souboru `mqwebuser.xml` .
- V 9.3.5 Linux Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Postup

1. Nainstalujte komponenty IBM MQ Console a REST API :
   - AIX V systému AIXnainstalujte sadu souborů `mqm.web.rte` . Další informace o instalaci sad souborů v systému AIXviz AIX instalační úlohy.
   - IBM i V systému IBM inainstalujte webovou komponentu. Chcete-li použít tuto funkci, musíte také nainstalovat systém zpráv a webové služby 5724L26 IBM MQ Java a předpoklady produktu 5770JV1 Java SE 8. Další informace o instalaci funkcí v systému IBM iviz IBM i instalační úlohy.
   - Linux V systému Linuxnainstalujte komponentu `MQSeriesWeb` . Další informace o instalaci komponent v systému Linuxnaleznete v části Linux instalační úlohy.

     V 9.3.5 V systému IBM MQ 9.3.5můžete také spustit server mqweb v samostatné IBM MQ Web Server instalaci na systému Linux. Další informace o instalaci konzoly IBM MQ Web Servernaleznete v tématu Instalace samostatného serveru IBM MQ Web Server.
   - Windows V systému Windowsnainstalujte funkci `Web Administration` . Další informace o instalaci funkcí v systému Windowsviz Windows instalační úlohy.
   - z/OS Nainstalujte funkci `IBM MQ for z/OS UNIX System Services Web Components` . Další informace o instalaci komponent a funkcí v systému z/OSviz z/OS instalační úlohy.
2. Vytvořte server mqweb, který je hostitelem IBM MQ Console a REST API.
   - z/OS V systému z/OSspusťte skript **`crtmqweb`** .

     Tento skript vytvoří uživatelský adresář WebSphere Liberty , který obsahuje konfiguraci serveru mqweb a soubory protokolu. Další informace o spuštění skriptu **`crtmqweb`** viz “Vytvoření serveru mqweb” na stránce 938.
   - V 9.3.5 Linux V samostatné instalaci produktu IBM MQ Web Server postupujte podle pokynů v části “Konfigurace samostatného serveru IBM MQ Web Server” na stránce 790.
   - Ve všech ostatních prostředích nemusíte provádět žádné akce k vytvoření serveru mqweb.

3. z/OS
   V systému z/OSvytvořte katalogizovaný postup pro spuštění serveru mqweb.
   Další informace viz téma “Vytvoření procedury pro server mqweb” na stránce 941.
4. Nahraďte existující konfigurační soubor `mqwebuser.xml` ukázkovým souborem základního registru, který je nakonfigurován tak, aby poskytoval základní zabezpečení. Zkopírujte soubor `basic_registry.xml` z adresáře *MQ_INSTALLATION_PATH*`/web/mq/samp/configuration` do příslušného adresáře vašeho systému a přejmenujte jej na `mqwebuser.xml`:
   - V instalaci produktu IBM MQ zkopírujte soubor do následujícího adresáře:
     - Linux AIX V systému AIX and Linux: `/var/mqm/web/installations/`*`installationName`*`/servers/mqweb`
     - Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*`\servers\mqweb`

       Kde *MQ_DATA_PATH* je cesta k datům IBM MQ , je tato cesta cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
     - z/OS V systému z/OS: *`WLP_user_directory`*`/servers/mqweb`

       Kde *WLP_user_directory* je adresář, který byl zadán při spuštění skriptu **crtmqweb** pro vytvoření definice serveru mqweb.
   - V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb`

     kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

   Ukázkový soubor `basic_registry.xml` konfiguruje čtyři uživatele:

   MQADMIN
   Administrativní uživatel, který je členem role `MQWebAdmin` .

   mqreader
   Administrativní uživatel jen pro čtení, který je členem role `MQWebAdminRO` .

   mftadmin
   Administrativní uživatel, který je členem role `MFTWebAdmin` .

   mftreader
   Administrativní uživatel jen pro čtení, který je členem role `MFTWebAdminRO` .

   Všichni uživatelé jsou také členy role `MQWebUser` .

   Další informace o dostupných rolích naleznete v tématu Role na portálech IBM MQ Console a REST API .
5. Volitelné: Upravte soubor `mqwebuser.xml` a přidejte další uživatele a skupiny. Přiřaďte těmto uživatelům a skupinám odpovídající role, které mají být autorizovány k použití REST API nebo IBM MQ Console. Můžete také změnit hesla pro uživatele, kteří jsou definováni jako výchozí, a zakódovat nová hesla. Další informace viz Konfigurace uživatelů a rolí.

   Poznámka:

   - z/OS Pokud v systému z/OSpřidáte uživatele do role `MQWebUser` , musíte také udělit ID uživatele spuštěné úlohy mqweb alternativnímu přístupu uživatele k ID uživatele s rolí `MQWebUser` . Příklad:

     ```
     RDEFINE MQADMIN hlq.ALTERNATE.USER.userId UACC(NONE)
     PERMIT hlq.ALTERNATE.USER.userId CLASS(MQADMIN) ACCESS(UPDATE) ID(mqwebUserId)
     ```

   - Multi z/OS Chcete-li dokončit kroky pro zahájení práce s produktem messaging REST API, musíte přidat uživatele do souboru `mqwebuser.xml` . Tento uživatel musí mít stejné

jméno jako existující uživatel IBM MQ ve vašem systému. Podle stejného formátu jako ostatní uživatelé v souboru XML přidejte ID uživatele a heslo za následující řádek v souboru XML: `<user name="mftreader" password="mftreader"/>`.

6. Nastavte prostředí tak, aby ukazovaly na konfiguraci serveru mqweb.
   - z/OS V systému z/OSnastavte proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb, zadáním následujícího příkazu:

     ```
     export WLP_USER_DIR=WLP_user_directory
     ```

     Kde *WLP_user_directory* je název adresáře, který je předán příkazu **crtmqweb** . Příklad:

     ```
     export WLP_USER_DIR=/var/mqm/web/installation1
     ```

     Další informace viz téma “Vytvoření serveru mqweb” na stránce 938.
   - V 9.3.5 Linux V samostatné instalaci produktu IBM MQ Web Server nastavte proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

     Pokud jste například zvolili použití `/var/mqweb` jako datový adresář IBM MQ Web Server , zadejte následující příkaz:

     ```
     export MQ_OVERRIDE_DATA_PATH=/var/mqweb
     ```
   - Ve všech ostatních prostředích nemusíte provádět žádné akce pro nastavení prostředí.
7. Standardně jsou volby REST API a IBM MQ Console k dispozici pouze ze stejného hostitele jako server mqweb. Povolte vzdálená připojení k serveru mqweb zadáním následujícího příkazu:

   ```
   setmqweb properties -k httpHost -v hostname
   ```

   Kde *název hostitele* uvádí adresu IP, název hostitele DNS (Domain Name Server) s příponou názvu domény nebo název hostitele DNS serveru, kde je nainstalován produkt IBM MQ . Chcete-li zadat všechna dostupná síťová rozhraní, použijte hvězdičku * v uvozovkách, jak ukazuje následující příklad:

   ```
   setmqweb properties -k httpHost -v "*"
   ```
8. Volitelné: Standardně není administrative REST API pro MFT povoleno. Chcete-li použít tuto funkci, musíte ji povolit a nakonfigurovat koordinačního správce front:
   a) Povolte administrative REST API pro MFT zadáním následujícího příkazu:

      ```
      setmqweb properties -k mqRestMftEnabled -v true
      ```

   b) Konfigurujte, který správce front je koordinačním správcem front, zadáním následujícího příkazu:

      ```
      setmqweb properties -k mqRestMftCoordinationQmgr -v qmgrName
      ```

      Kde *qmgrName* je název koordinačního správce front.

   c) Chcete-li povolit volání POST, konfigurujte správce front, který je správcem front příkazů, zadáním následujícího příkazu:

      ```
      setmqweb properties -k mqRestMftCommandQmgr -v qmgrName
      ```

      Kde *qmgrName* je název správce front příkazů.
9. Spusťte server mqweb, který podporuje REST API a IBM MQ Console:
   - ALW V systému AIX, Linux, and Windowszadejte jako privilegovaný uživatelnásledující příkaz:

     ```
     strmqweb
     ```

- IBM i V systému IBM izadejte jako privilegovaný uživatelv prostředí Qshell následující příkaz:

  ```
  /QIBM/ProdData/mqm/bin/strmqweb
  ```

- z/OS V systému z/OSspusťte proceduru, kterou jste vytvořili v adresáři “Vytvoření procedury pro server mqweb” na stránce 941.

  Následující zprávy jsou vydány pro STDOUT DD, aby označily, že server mqweb byl úspěšně spuštěn.

  ```
  [AUDIT   ] MQWB2019I: MQ Console level: 9.2.4 - V924-CD924-L211028
  [AUDIT   ] MQWB0023I: MQ REST API level: 9.2.4 - V924-CD924-L211028
  [AUDIT   ] CWWKZ0001I: Application com.ibm.mq.rest started in 1.763 seconds.
  [AUDIT   ] CWWKZ0001I: Application com.ibm.mq.console started in 2.615 seconds.
  [AUDIT   ] CWWKF0011I: The mqweb server is ready to run a smarter planet. The mqweb
  server started in 10.016 seconds.
  ```

Server mqweb můžete kdykoli zastavit zastavením spuštěné úlohy serveru mqweb v systému z/OSnebo pomocí příkazu **endmqweb** . Pokud však server mqweb není spuštěn, nemůžete použít REST API nebo IBM MQ Console.

10. z/OS

    Volitelné: Chcete-li v systému z/OSpovolit produktům pro automatizaci systému zachycovat zprávy MQWB2019I a MQWB0023I , které jsou vydány při spuštění IBM MQ Console a REST API , nakonfigurujte server mqweb tak, aby tyto zprávy zapisoval do konzoly MVS . Chcete-li nakonfigurovat server mqweb pro zápis zpráv MQWB2019I a MQWB0023I do konzoly MVS , upravte soubor `mqwebuser.xml` , který jste vytvořili v kroku “4” na stránce 788, a přidejte do souboru následující řádek:

    ```
    <zosLogging enableLogToMVS="true" wtoMessage="MQWB2019I,MQWB0023I"/>
    ```

    Další informace o konfiguraci z/OS Protokolování na serveru mqweb viz z/OS Protokolování (zosLogging).

Jak pokračovat dále

1. Nakonfigurujte nastavení serveru mqweb, včetně povolení připojení HTTP , a změňte číslo portu. Další informace viz téma “Konfigurace IBM MQ Console a REST API” na stránce 786.
2. Volitelně nakonfigurujte REST API:
   a. Nakonfigurujte sdílení prostředků mezi zdroji pro REST API. Standardně nemůžete přistupovat k serveru REST API z webových prostředků, které nejsou hostovány ve stejné doméně jako server REST API. To znamená, že požadavky na křížový původ nejsou povoleny. Můžete konfigurovat sdílení CORS (Cross Origin Resource Sharing), abyste povolili požadavky na křížový původ z určených adres URL. Další informace viz Konfigurace CORS pro REST API.
   b. Nakonfigurujte REST API pro MFT. Další informace viz téma “Konfigurace REST API pro MFT” na stránce 811.
3. Použijte REST API nebo IBM MQ Console:
   - Začínáme s produktem administrative REST API
   - Začínáme s produktem messaging REST API
   - Začínáme s produktem IBM MQ Console

V 9.3.5 Linux Konfigurace samostatného serveru IBM MQ Web Server

V produktu IBM MQ 9.3.5můžete spustit server mqweb, který hostuje IBM MQ Console a REST API v samostatné instalaci produktu IBM MQ Web Server .

Než začnete

Samostatný soubor IBM MQ Web Server je k dispozici pouze v systému Linux.

Než budete moci konfigurovat server mqweb, musíte nainstalovat produkt IBM MQ Web Server podle pokynů v části Instalace samostatného serveru IBM MQ Web Server.

Informace o této úloze

Postupujte podle pokynů v této úloze a vytvořte a nakonfigurujte nový server mqweb, který se spustí v samostatné instalaci produktu IBM MQ Web Server . Opakováním tohoto postupu můžete nakonfigurovat více než jeden server mqweb pro spuštění v samostatné instalaci produktu IBM MQ Web Server .

Postup

1. Vytvořte datový adresář IBM MQ Web Server .

   Datový adresář se používá k uložení konfiguračních souborů a souborů protokolu pro server mqweb, na kterém jsou spuštěny soubory IBM MQ Console a REST API. Můžete použít libovolný adresář, který vyberete jako datový adresář IBM MQ Web Server .

   ID uživatele, které používáte ke spuštění serveru mqweb, musí mít udělen přístup pro čtení a zápis k datovému adresáři.
2. Nastavte proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář, který jste vytvořili v kroku “1” na stránce 791.
   Pokud jste například zvolili použití `/var/mqweb` jako datový adresář IBM MQ Web Server , zadejte následující příkaz:

   ```
   export MQ_OVERRIDE_DATA_PATH=/var/mqweb
   ```
3. Pomocí příkazu **setmqenv** nastavte prostředí IBM MQ .

   Přejděte do adresáře `bin` instalačního adresáře IBM MQ Web Server a zadejte následující příkaz:

   ```
   . setmqenv -s
   ```
4. Pomocí příkazu **crtmqdir** vytvořte adresáře a soubory IBM MQ v datovém adresáři. Vytvořené soubory zahrnují definici šablony pro server mqweb.

   Spusťte následující příkaz:

   ```
   crtmqdir -s -f
   ```
5. Volitelné: Pokud je tento server mqweb prvním serverem, který jste vytvořili pro spuštění s touto instalací samostatného serveru IBM MQ Web Server, použijte příkaz **mqlicense** ke kontrole a přijetí licence IBM MQ .

   Tento příkaz musíte spustit jako uživatel, který má přístup pro zápis do instalačního adresáře IBM MQ Web Server .

   Chcete-li například zobrazit licenci IBM MQ , zadejte následující příkaz:

   ```
   mqlicense
   ```

   Další informace viz mqlicense.
6. Volitelné: Chcete-li migrovat existující server mqweb pro spuštění v nově nakonfigurované samostatné instalaci produktu IBM MQ Web Server , postupujte takto:

   a. Zazálohujte existující konfiguraci serveru mqweb.

   b. Obnovte soubory do adresáře *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST` , kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , který jste vytvořili v kroku “1” na stránce 791.

   Další informace viz téma “Zálohování a obnova konfigurace serveru mqweb” na stránce 820.

Poznámka: Některé funkce IBM MQ Console a REST API nejsou k dispozici v samostatné instalaci produktu IBM MQ Web Server . Pokud migrujete server mqweb z instalace IBM MQ na samostatnou instalaci IBM MQ Web Server , tyto funkce nelze po migraci použít. Další informace o omezeních, která platí v samostatné instalaci produktu IBM MQ Web Server , naleznete v části IBM MQ Console a REST API.

Jak pokračovat dále

Nakonfigurujte server mqweb podle kroků popsaných v tématu “Základní konfigurace pro server mqweb” na stránce 787.

Konfigurace zabezpečení

Můžete nakonfigurovat zabezpečení pro IBM MQ Console a REST API úpravou souboru `mqwebuser.xml` . Uživatele můžete nakonfigurovat a ověřit tak, že nakonfigurujete buď základní registr uživatelů, registr LDAP, nebo jakýkoli jiný typ registru, který je poskytován s produktem WebSphere Liberty. Poté můžete tyto uživatele autorizovat přiřazením uživatelů a skupin k roli.

Informace o této úloze

Chcete-li nakonfigurovat zabezpečení pro IBM MQ Consolea REST API, musíte nakonfigurovat uživatele a skupiny. Tito uživatelé a skupiny pak mohou být autorizováni používat IBM MQ Console, REST APInebo obojí. Další informace o konfiguraci uživatelů a skupin a ověřování a autorizaci uživatelů naleznete v části IBM MQ Console a REST API zabezpečení.

Když se uživatelé ověřují s produktem IBM MQ Console, vygeneruje se token LTPA. Tento token umožňuje uživateli používat IBM MQ Console bez opětovného ověření, dokud token nevyprší.

Pokud používáte ověření založené na tokenech s produktem REST API, vygeneruje se jiný token LTPA, když se uživatel přihlásí pomocí prostředku `/login` REST API pomocí metody HTTP POST. Můžete nakonfigurovat, kdy vyprší platnost tohoto tokenu, a zda lze tento token použít pro připojení HTTP i HTTPS . Další informace viz “Konfigurace tokenu LTPA” na stránce 800.

Procedura

- IBM MQ Console a REST API zabezpečení
- “Konfigurace tokenu LTPA” na stránce 800

Konfigurace názvu hostitele HTTP

Standardně je server mqweb, který hostuje IBM MQ Console a REST API , nakonfigurován tak, aby povoloval pouze lokální připojení. To znamená, že k IBM MQ Console a REST API lze přistupovat pouze na systému, na kterém jsou nainstalovány produkty IBM MQ Console a REST API . Název hostitele můžete nakonfigurovat tak, aby umožňoval vzdálená připojení, pomocí příkazu **setmqweb** .

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do crtmqweb. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Upozornění: Linux V 9.3.5

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v samostatné instalaci produktu IBM MQ Web Server musíte nastavit proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

Procedura

- Zobrazte aktuální konfiguraci názvu hostitele HTTP pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole httpHost zobrazuje název hostitele HTTP .
- Nastavte název hostitele HTTP pomocí následujícího příkazu:

  ```
  setmqweb properties -k httpHost -v hostName
  ```

  kde *hostName* uvádí adresu IP, název hostitele DNS (Domain Name Server) s příponou názvu domény nebo název hostitele DNS serveru, na kterém je nainstalován produkt IBM MQ . Chcete-li uvést všechna dostupná síťová rozhraní, použijte hvězdičku v uvozovkách. Chcete-li povolit pouze lokální připojení, použijte hodnotu localhost .
- Zrušte nastavení názvu hostitele HTTP pomocí následujícího příkazu:

  ```
  setmqweb properties -k httpHost -d
  ```

Konfigurace portů HTTP a HTTPS

Standardně server mqweb, který je hostitelem IBM MQ Console a REST API , používá port HTTPS 9443. Port, který je přidružen k připojením HTTP , je zakázán. Můžete povolit port HTTP , nakonfigurovat jiný port HTTPS nebo zakázat port HTTP nebo HTTPS . Porty můžete nakonfigurovat pomocí příkazu **setmqweb** .

Než začnete

Pokud povolíte port HTTP a používáte ověřování založené na tokenech, musíte povolit použití stejného tokenu LTPA pro připojení HTTP i HTTPS . Další informace viz téma “Konfigurace tokenu LTPA” na stránce 800.

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru mqwebuser.xml .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru mqwebuser.xml v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Upozornění: Linux V 9.3.5

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v samostatné instalaci produktu IBM MQ Web Server musíte nastavit proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

Upozornění: Standardně server mqweb vyžaduje, aby byly tokeny LTPA zabezpečeny pro všechny požadavky. Pokud je server mqweb nakonfigurován tak, aby vyžadoval zabezpečení tokenů LTPA, nemůžete při připojení k portu HTTP provést následující akce:

- Přihlaste se ke konzole IBM MQ Console.
- Použijte ověření založené na tokenech s REST API.

Chcete-li povolit použití tokenů LTPA požadavky HTTP , nastavte hodnotu vlastnosti **secureLTPA** na `false`. Další informace viz téma “Konfigurace tokenu LTPA” na stránce 800.

Procedura

- Zobrazte aktuální konfiguraci portů HTTP a HTTPS pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `httpPort` zobrazuje port HTTP a pole `httpsPort` zobrazuje port HTTPS .
- Povolte nebo nakonfigurujte port HTTP : pomocí následujícího příkazu:
  - Povolte nebo nastavte port HTTP pomocí následujícího příkazu:

    ```
    setmqweb properties -k httpPort -v portNumber
    ```

    kde *portNumber* uvádí port, který chcete použít pro připojení HTTP . Port můžete zakázat pomocí hodnoty `-1`.
  - Pomocí následujícího příkazu resetujte hodnotu portu HTTP na výchozí hodnotu `-1` :

    ```
    setmqweb properties -k httpPort -d
    ```
- Nakonfigurujte port HTTPS :
  - Nastavte číslo portu HTTPS pomocí následujícího příkazu:

    ```
    setmqweb properties -k httpsPort -v portNumber
    ```

    kde *portNumber* uvádí port, který chcete použít pro připojení HTTPS . Port můžete zakázat pomocí hodnoty `-1`.
  - Pomocí následujícího příkazu resetujte číslo portu HTTPS na výchozí hodnotu 9443 :

    ```
    setmqweb properties -k httpsPort -d
    ```

Konfigurace časového limitu odezvy

Standardně vyprší časový limit IBM MQ Console a REST API , pokud je doba potřebná k odeslání odpovědi zpět klientovi delší než 30 sekund. Můžete nakonfigurovat IBM MQ Console a REST API tak, aby používaly jinou hodnotu časového limitu, pomocí příkazu **setmqweb** .

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Upozornění: Linux V 9.3.5

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v samostatné instalaci produktu IBM MQ Web Server musíte nastavit proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

Procedura

- Zobrazte aktuální konfiguraci časového limitu požadavku pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestRequestTimeout` zobrazuje aktuální hodnotu časového limitu odezvy. Další informace viz dspmqweb properties.
- Nastavte časový limit požadavku pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestRequestTimeout -v timeout
  ```

  kde *timeout* určuje čas v sekundách před vypršením časového limitu.
- Pomocí následujícího příkazu resetujte časový limit požadavku na výchozí hodnotu 30 sekund:

  ```
  setmqweb properties -k mqRestRequestTimeout -d
  ```

Konfigurace automatického spuštění

Standardně se IBM MQ Console automaticky spustí při spuštění serveru mqweb. Pomocí příkazu **setmqweb** můžete nakonfigurovat, zda se IBM MQ Console a REST API automaticky spustí.

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Upozornění: Linux V 9.3.5

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v samostatné instalaci produktu IBM MQ Web Server musíte nastavit proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

Procedura

- Zobrazte aktuální konfiguraci automatického spuštění pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestAutostart` zobrazuje, zda je produkt REST API automaticky spuštěn, a pole `mqConsoleAutostart` zobrazuje, zda je produkt IBM MQ Console automaticky spuštěn.
- Nakonfigurujte, zda se IBM MQ Console spustí automaticky, pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqConsoleAutostart -v start
  ```

  kde *start* je hodnota `true` , pokud chcete, aby se IBM MQ Console automaticky spustil, nebo `false` jinak.
- Nakonfigurujte, zda se REST API spustí automaticky, pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestAutostart -v start
  ```

  kde *start* je hodnota `true` , pokud chcete, aby se REST API automaticky spustil, nebo `false` jinak.

Konfigurace protokolování

Můžete konfigurovat úrovně protokolování, maximální velikost souboru protokolu a maximální počet souborů protokolu používaných serverem mqweb, který je hostitelem serverů IBM MQ Console a REST API. Protokolování můžete konfigurovat pomocí příkazu **setmqweb** .

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Upozornění: Linux V 9.3.5

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v samostatné instalaci produktu IBM MQ Web Server musíte nastavit proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

Informace o této úloze

Server mqweb zapisuje zprávy protokolu a trasování do následujících souborů protokolu:

`console.log` a `messages.log`
Tyto soubory obsahují zprávy vydané serverem IBM MQ Console, serverem REST APIa serverem mqweb, který spouští tyto komponenty.

`trace.log`
Tento soubor obsahuje trasování pro IBM MQ Console a REST API. Trasování se do tohoto souboru zapisuje pouze v případě, že je povoleno trasování.

Soubory protokolu pro server mqweb lze nalézt v jednom z následujících adresářů:

- V instalaci produktu IBM MQ :
  - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*`installationName`*`/servers/mqweb/logs`
  - Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*`\servers\mqweb\logs`, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
  - z/OS V systému z/OS: *WLP_user_directory*`/servers/mqweb/logs`

    kde *WLP_user_directory* je adresář určený při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.

- V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*/web/installations/MQWEBINST/servers/mqweb/logs

  kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

Soubory trasování systému zpráv pro kód systému zpráv REST API , který je spuštěn na serveru mqweb, lze nalézt v jednom z následujících adresářů:

- V instalaci produktu IBM MQ :
  - Linux AIX V systému AIX nebo Linux: /var/mqm/web/installations/*installationName*/servers/mqweb
  - Windows V systému Windows: *MQ_DATA_PATH*\web\installations*installationName*\servers\mqweb, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta C:\ProgramData\IBM\MQ.
  - z/OS V systému z/OS: *WLP_user_directory*/servers/mqweb

    kde *WLP_user_directory* je adresář určený při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.
- V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*/web/installations/MQWEBINST/servers/mqweb

  kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

Další informace o povolení trasování pro:

- REST API, viz Trasování REST API
- IBM MQ Console, viz Trasování IBM MQ Console

Procedura

- Zobrazte aktuální konfiguraci protokolování REST API pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  - Pole maxTraceFileSize zobrazuje maximální velikost souboru protokolu
  - Pole maxTraceFiles zobrazuje maximální počet souborů protokolu
  - Pole traceSpec zobrazuje použitou úroveň trasování.
  - Pole maxMsgTraceFileSize zobrazuje maximální velikost trasovacího souboru systému zpráv.
  - Pole maxMsgTraceFiles zobrazuje maximální počet souborů trasování systému zpráv.
- Nakonfigurujte maximální velikost souborů messages.log a trace.log :
  - Nastavte maximální velikost souboru protokolu pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxTraceFileSize -v size
    ```

    kde *velikost* uvádí velikost v MB, kterou může každý soubor protokolu dosáhnout.
  - Pomocí následujícího příkazu resetujte maximální velikost souboru protokolu na výchozí hodnotu 20 MB:

    ```
    setmqweb properties -k maxTraceFileSize -d
    ```
- Nakonfigurujte maximální počet souborů messages.log a trace.log :
  - Nastavte maximální počet jednotlivých souborů protokolu pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxTraceFiles -v max
    ```

kde *max* uvádí maximální počet souborů.

- Pomocí následujícího příkazu resetujte maximální počet jednotlivých souborů protokolu na výchozí hodnotu 2:

  ```
  setmqweb properties -k maxTraceFiles -d
  ```

- Nakonfigurujte maximální velikost trasovacího souboru systému zpráv:
  - Nastavte maximální velikost trasovacího souboru systému zpráv pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxMsgTraceFileSize -v size
    ```

    kde *size* určuje velikost v MB, kterou může dosáhnout každý trasovací soubor systému zpráv.
  - Pomocí následujícího příkazu resetujte maximální velikost trasovacího souboru systému zpráv na výchozí hodnotu 200 MB:

    ```
    setmqweb properties -k maxMsgTraceFileSize -d
    ```

- Nakonfigurujte maximální počet trasovacích souborů systému zpráv, které se mají použít:
  - Nastavte maximální počet souborů, které se mají použít pro trasování systému zpráv, pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxMsgTraceFiles -v max
    ```

    kde *max* uvádí maximální počet souborů.
  - Pomocí následujícího příkazu resetujte maximální počet souborů, které se mají použít pro trasování systému zpráv, na výchozí hodnotu 5:

    ```
    setmqweb properties -k maxMsgTraceFiles -d
    ```

- Nakonfigurujte úroveň trasování, kterou server mqweb zapisuje:
  - Nastavte specifikaci trasování, která se používá, pomocí následujícího příkazu:

    ```
    setmqweb properties -k traceSpec -v level
    ```

    kde *úroveň* je jedna z hodnot, které jsou uvedeny v seznamu Tabulka 51 na stránce 799. Tabulka nastiňuje úrovně protokolování, seřazené podle zvyšující se úrovně podrobností. Když povolíte úroveň protokolování, povolíte také každou úroveň před ní. Pokud například povolíte úroveň protokolování ***=warning** , povolíte také úrovně protokolování ***=severe**a ***=fatal** .

    Tuto hodnotu změňte na žádost podpory IBM .
  - Resetujte specifikaci trasování, která se používá na výchozí hodnotu ***=info** , pomocí následujícího příkazu:

    ```
    setmqweb properties -k traceSpec -d
    ```

Tabulka 51. Platné úrovně protokolování

Hodnota	**Použitá úroveň protokolování**
* =vypnuto	Protokolování je vypnuto.
* =fatální	Úloha nemůže pokračovat a komponenta, aplikace a server nemohou fungovat.
* =závažné	Úloha nemůže pokračovat, ale komponenta, aplikace a server mohou stále fungovat. Tato úroveň může také označovat hrozící neopravitelnou chybu.
* =varování	Potenciální chyba nebo hrozící chyba. Tato úroveň může také označovat progresivní selhání (například potenciální úniku prostředků).
* =audit	Významná událost ovlivňující stav serveru nebo prostředky

Tabulka 51. Platné úrovně protokolování (pokračování)	
Hodnota	**Použitá úroveň protokolování**
* =info	Obecné informace nastiňující celkový průběh úlohy
* =konfigurace	Změna nebo stav konfigurace
* =podrobnost	Obecné informace o průběhu dílčí úlohy
* =v pořádku	Informace o trasování-Obecné informace o trasování + zadání metody, ukončení a návratové hodnoty
* =jemnější	Informace o trasování-podrobné trasování
* =nejjemnější	Informace o trasování-podrobnější trasování, které zahrnuje všechny podrobnosti potřebné k ladění problémů.
* =vše	Všechny události jsou protokolovány

Konfigurace tokenu LTPA

Tokeny LTPA lze použít, chcete-li se vyhnout tomu, aby uživatel při každém požadavku na server mqweb zadal pověření pro jméno uživatele a heslo. Pomocí příkazu **setmqweb** můžete konfigurovat název souboru cookie tokenu LTPA, interval vypršení platnosti pro tokeny ověřování LTPA a zda lze tokeny LTPA používat pro připojení HTTP .

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Poznámka: Používáte-li ověření tokenu IBM MQ Consolei ověření tokenu s produktem REST API, bude interval vypršení platnosti sdílen.

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Upozornění: Linux V 9.3.5

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v samostatné instalaci produktu IBM MQ Web Server musíte nastavit proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

Informace o této úloze

Když se uživatelé přihlásí k serveru IBM MQ Console, vygeneruje se token LTPA. Pokud použijete ověření založené na tokenech s produktem REST API, vygeneruje se token LTPA, když se uživatel přihlásí pomocí prostředku `/login` REST API pomocí metody HTTP POST. Tento token je vrácen v souboru cookie. Token se používá k ověření uživatele, aniž by se musel znovu přihlásit se svým ID uživatele a heslem, dokud token nevyprší. Výchozí interval vypršení platnosti je 120 minut.

Název souboru cookie, který obsahuje token LTPA, se liší podle platformy:

- MQ Appliance V systému IBM MQ Applianceje token LTPA `LtpaToken2`. Tuto hodnotu nelze změnit.
- z/OS ALW Ve výchozím nastavení na všech ostatních platformách název souboru cookie, který obsahuje token LTPA, začíná řetězcem `LtpaToken2`a obsahuje příponu, kterou lze změnit při restartování serveru mqweb. Tento náhodný název souboru cookie umožňuje spuštění více než jednoho serveru mqweb na stejném systému. Pokud však chcete, aby název souboru cookie zůstal konzistentní hodnotou, můžete zadat název, který má soubor cookie, pomocí příkazu **setmqweb** .

z/OS IBM i ALW Pokud povolíte oba porty HTTP a HTTPS , token LTPA, který je vydán pro požadavek HTTPS , lze znovu použít pro požadavek HTTP . Toto chování je standardně zakázáno, ale toto chování můžete povolit pomocí příkazu **setmqweb** .

Procedura

- Zobrazte aktuální vypršení platnosti tokenu LTPA, název souboru cookie tokenu LTPA a zda lze token LTPA použít pro požadavky HTTP pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  - Pole `ltpaCookieName` zobrazuje název souboru cookie tokenu LTPA. Pokud jste nenastavili název souboru cookie, hodnota této vlastnosti je `LtpaToken2_${env.MQWEB_LTPA_SUFFIX}` on AIX, Linux, and Windows nebo `LtpaToken2_${httpsPort}` on z/OS, . Proměnnou za předponou `LtpaToken2_` používá server mqweb k vygenerování jedinečného názvu pro soubor cookie. Tuto proměnnou nemůžete nastavit, ale můžete změnit `ltpaCookieName` na hodnotu, kterou si zvolíte.
  - Pole `ltpaExpiration` zobrazuje čas vypršení platnosti tokenu LTPA.
  - Pole `secureLtpa` je nastaveno na hodnotu `false` , pokud mohou být tokeny LTPA použity požadavky HTTP .
- Nakonfigurujte vypršení platnosti tokenu LTPA:
  - Nastavte vypršení platnosti tokenu LTPA zadáním následujícího příkazu:

    ```
    setmqweb properties -k ltpaExpiration -v time
    ```

    kde *čas* určuje čas v minutách před vypršením platnosti tokenu LTPA a odhlášením uživatele.
  - Resetujte vypršení platnosti tokenu LTPA na výchozí hodnotu 120 minut zadáním následujícího příkazu:

    ```
    setmqweb properties -k ltpaExpiration -d
    ```
- z/OS ALW

  Nakonfigurujte název souboru cookie tokenu LTPA:
  - Nastavte název souboru cookie tokenu LTPA zadáním následujícího příkazu:

    ```
    setmqweb properties -k ltpaCookieName -v name
    ```

    kde *name* určuje jedinečný název pro soubor cookie tokenu LTPA.

- Resetujte název souboru cookie tokenu LTPA na výchozí hodnotu, kde za předponou `LtpaToken2_` následují náhodné znaky, zadáním následujícího příkazu:

  ```
  setmqweb properties -k ltpaCookieName -d
  ```

- z/OS ALW

  Nakonfigurujte, zda může token LTPA používat připojení HTTP , zadáním následujícího příkazu:

  ```
  setmqweb properties -k secureLtpa -v secure
  ```

  kde *secure* určuje, zda může být token LTPA používán jak nezabezpečenými připojeními HTTP , tak zabezpečenými připojeními HTTPS . Hodnota `false` umožňuje připojení HTTP i HTTPS používat stejný token LTPA.

V 9.3.0 Konfigurace chování připojení vzdáleného správce front pro IBM MQ Console

Při použití konzoly IBM MQ Consolemůžete vytvářet připojení ke vzdáleným správcům front. To znamená, že se můžete připojit ke správcům front, kteří nejsou součástí stejné instalace jako server mqweb, na kterém běží produkt IBM MQ Console. Existuje řada voleb konfigurace, které lze nastavit pro řízení chování připojení vzdáleného správce front.

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Upozornění: Linux V 9.3.5

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v samostatné instalaci produktu IBM MQ Web Server musíte nastavit proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .

Informace o této úloze

Můžete nastavit následující volby konfigurace:

- Zda jsou povolena připojení vzdáleného správce front.

- Zda lze připojení přidat pomocí IBM MQ Console, nebo pouze pomocí příkazového řádku.
- Určuje, zda jsou v produktu IBM MQ Console zobrazeni lokální správci front, jsou-li povolena připojení vzdáleného správce front.
- Určuje, zda jsou připojení vzdáleného správce front automaticky vytvořena při spuštění konzoly IBM MQ Console nebo při selhání připojení.
- Doba mezi jednotlivými aktualizacemi seznamu vzdálených správců front zobrazenými v souboru IBM MQ Console.

Procedura

- Chcete-li zobrazit aktuální nastavení konfigurace připojení vzdáleného správce front, zadejte následující příkaz:

  ```
  dspmqweb properties -a
  ```

  - V poli `mqConsoleRemoteSupportEnabled` je uvedeno, zda jsou povolena připojení vzdáleného správce front.
  - V poli `mqConsoleRemoteUIAdmin` je uvedeno, zda lze připojení vzdáleného správce front přidat pomocí konzoly IBM MQ Console.
  - V poli `mqConsoleRemoteAllowLocal` je uvedeno, zda jsou zobrazeni lokální správci front.
  - V poli `mqConsoleRemotePollTime` je uveden počet sekund mezi jednotlivými aktualizacemi seznamu vzdálených správců front.
- Chcete-li zabránit nebo povolit připojení vzdáleného správce front s produktem IBM MQ Console, zadejte následující příkaz:

  ```
  setmqweb properties -k mqConsoleRemoteSupportEnabled -v true or false
  ```

  kde hodnota *true* povoluje připojení vzdáleného správce front nebo hodnota `false` zabraňuje připojení vzdáleného správce front.

  Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , vlastnost **mqConsoleRemoteSupportEnabled** není platná. Samostatný produkt IBM MQ Web Server podporuje připojení pouze ke vzdáleným správcům front.
- Chcete-li zabránit nebo povolit přidání připojení vzdáleného správce front pomocí konzoly IBM MQ Consolenebo pouze pomocí příkazového řádku, zadejte následující příkaz:

  ```
  setmqweb properties -k mqConsoleRemoteUIAdmin -v true or false
  ```

  kde parametr `true` umožňuje přidání připojení vzdáleného správce front pomocí konzoly IBM MQ Console a příkazového řádku nebo parametr `false` umožňuje přidání připojení vzdáleného správce front pouze pomocí příkazu **setmqweb remote** na příkazovém řádku.
- Chcete-li zabránit nebo povolit zobrazení lokálních správců front v produktu IBM MQ Console v případě, že jsou povolena vzdálená připojení správce front, zadejte následující příkaz:

  ```
  setmqweb properties -k mqConsoleRemoteAllowLocal -v true or false
  ```

  kde `true` umožňuje zobrazení lokálních správců front nebo `false` skryje lokální správce front.

  Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , vlastnost **mqConsoleRemoteAllowLocal** není platná. Samostatný produkt IBM MQ Web Server podporuje připojení pouze ke vzdáleným správcům front.
- Chcete-li nastavit dobu mezi jednotlivými aktualizacemi seznamu vzdálených správců front zobrazených v produktu IBM MQ Console, zadejte následující příkaz:

  ```
  setmqweb properties -k mqConsoleRemotePollTime -v seconds
  ```

  kde hodnota *seconds* je nastavena na celočíselnou hodnotu počtu sekund mezi jednotlivými aktualizacemi seznamu vzdálených správců front.

Související odkazy
setmqweb
dspmqweb

Konfigurace brány administrative REST API

Je-li povolena brána administrative REST API , můžete provádět vzdálenou administraci s produktem REST API pomocí správce front brány. Můžete nakonfigurovat správce front, který se používá jako výchozí správce front brány, nebo můžete zabránit vzdálené administraci zakázáním brány administrative REST API pomocí příkazu **setmqweb** .

Než začnete

Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , nelze tuto úlohu použít. Produkt administrative REST API není k dispozici v samostatné instalaci produktu IBM MQ Web Server .

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Informace o této úloze

Když je server mqweb spuštěn v instalaci produktu IBM MQ , brána administrative REST API je standardně povolena.

Výchozí správce front brány se používá v případě, že jsou splněny obě následující podmínky:

- V záhlaví `ibm-mq-rest-gateway-qmgr` požadavku REST není uveden správce front.
- Správce front určený v adrese URL prostředku REST API není lokálním správcem front.

Další informace o vzdálené administraci pomocí konzoly REST APInaleznete v tématu Vzdálená administrace pomocí konzoly REST API.

Procedura

- Zobrazte aktuální konfiguraci brány administrative REST API pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestGatewayEnabled` zobrazuje, zda je brána povolena, a pole `mqRestGatewayQmgr` zobrazuje název výchozího správce front brány.
- Nakonfigurujte, zda je brána administrative REST API povolena, pomocí následujícího příkazu:

```
setmqweb properties -k mqRestGatewayEnabled -v enabled
```

kde *enabled* je hodnota **true** , která povolí bránu administrative REST API , nebo **false** jinak.

- Konfigurujte, který správce front má být použit jako výchozí správce front brány:
  - Nastavte výchozího správce front brány pomocí následujícího příkazu:

    ```
    setmqweb properties -k mqRestGatewayQmgr -v qmgrName
    ```

    kde *qmgrName* je název správce front ve stejné instalaci jako server mqweb.
  - Zrušte nastavení výchozího správce front brány pomocí následujícího příkazu:

    ```
    setmqweb properties -k mqRestGatewayQmgr -d
    ```

Konfigurace agenta messaging REST API

messaging REST API můžete nakonfigurovat několika způsoby. Můžete se rozhodnout funkci messaging REST API povolit nebo zakázat. Můžete zvolit maximální počet připojení ve fondu, která mohou být použita produktem messaging REST API, a chování agenta messaging REST API , když jsou všechna připojení používána. Můžete také zvolit, jaký kontext uživatele se použije pro autorizaci, když používáte produkt messaging REST API k odeslání, přijetí, procházení nebo publikování zprávy.

Procedura

- “Povolení messaging REST API” na stránce 805
- “Konfigurace sdružování připojení pro messaging REST API” na stránce 806
- V 9.3.2 “Konfigurace kontextu uživatele, který se používá pro autorizaci v produktu messaging REST API” na stránce 809

Povolení messaging REST API

Můžete nakonfigurovat, zda je messaging REST API povolen, pomocí příkazu **setmqweb** . Standardně je messaging REST API povolen.

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Procedura

- Zobrazte aktuální konfiguraci serveru messaging REST API pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestMessagingEnabled` zobrazuje, zda je povolena volba messaging REST API . Je-li hodnota `True` , je povolena hodnota messaging REST API .
- Povolte messaging REST API pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingEnabled -v true
  ```
- Zakažte messaging REST API pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingEnabled -v false
  ```

Související úlohy

“Konfigurace sdružování připojení pro messaging REST API” na stránce 806
Můžete nakonfigurovat maximální počet připojení ve fondu, která mohou být použita produktem messaging REST API, a chování agenta messaging REST API , když jsou všechna připojení používána.

“Konfigurace kontextu uživatele, který se používá pro autorizaci v produktu messaging REST API” na stránce 809
V 9.3.2 Můžete nakonfigurovat, jaký uživatelský kontext se používá pro autorizaci, když používáte produkt messaging REST API k odeslání, přijetí, procházení nebo publikování zprávy. To znamená, že můžete zvolit, zda se pro autorizaci použije uživatel, který je přihlášen k serveru messaging REST API, nebo uživatel, který spustil server mqweb.

“Konfigurace režimu připojení pro messaging REST API” na stránce 808
Produkt messaging REST API můžete nakonfigurovat tak, aby se připojoval k lokálním nebo vzdáleným správcům front.

Konfigurace sdružování připojení pro messaging REST API

Můžete nakonfigurovat maximální počet připojení ve fondu, která mohou být použita produktem messaging REST API, a chování agenta messaging REST API , když jsou všechna připojení používána.

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do crtmqweb. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Informace o této úloze

Chcete-li optimalizovat výkon konzoly messaging REST API, jsou připojení ke správcům front produktu IBM MQ uložena ve fondu. To znamená, že místo každého požadavku REST, který vytváří, používá a odstraňuje vlastní připojení, používá každý požadavek REST připojení z fondu připojení. Standardně je pro každý fond správců front k dispozici 20 připojení a můžete si vybrat ze tří voleb pro zpracování požadavků, když jsou všechna připojení používána:

- Produkt messaging REST API může vytvořit nové připojení mimo fond, které se použije pro požadavek. Toto chování je výchozí.
- messaging REST API může vrátit chybu.
- Agent messaging REST API může čekat na zpřístupnění připojení ve fondu. Toto čekání je neurčité.

Pomocí příkazu **setmqweb properties** můžete změnit maximální počet připojení ve fondu a výchozí chování messaging REST API , když jsou všechna připojení používána.

Procedura

- Zobrazte aktuální konfiguraci pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  – Pole mqRestMessagingFullPoolBehavior zobrazuje chování agenta messaging REST API , když jsou všechna připojení ve fondu používána. Je-li hodnota block, musí agent messaging REST API čekat na dostupnost připojení. Pokud je hodnota error, messaging REST API musí vrátit chybu. Pokud je hodnota overflow, musí agent messaging REST API vytvořit připojení mimo fond, které se má použít, a po použití toto připojení zlikvidovat.

  – Pole mqRestMessagingMaxPoolSize zobrazuje maximální velikost fondu připojení.
- Nakonfigurujte chování agenta messaging REST API , když jsou všechna připojení ve fondu používána, pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingFullPoolBehavior -v action
  ```

  kde *akce* uvádí akci, která se má provést. *action* může mít jednu z následujících hodnot:

  blok
  Když jsou všechna připojení ve fondu používána, počkejte, až bude připojení k dispozici.

  Chyba
  Když jsou všechna připojení ve fondu používána, vrátí chybu.

  Přetečení
  Jsou-li všechna připojení ve fondu používána, vytvořte připojení, které není ve fondu, a po jeho použití připojení zlikvidujte.
- Konfigurujte maximální velikost fondu připojení pro každý fond správců front pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingMaxPoolSize -v size
  ```

  kde *size* určuje velikost fondu.

  Poznámka: Pokud je nastavena velká hodnota *mqRestMessagingMaxPoolSize* a je připojeno mnoho správců front, zvažte zvýšení maximální velikosti haldy serveru mqweb. Další informace naleznete v tématu vyladění prostředí JVM serveru mqweb .

Související úlohy

“Povolení messaging REST API” na stránce 805
Můžete nakonfigurovat, zda je messaging REST API povolen, pomocí příkazu **setmqweb** . Standardně je messaging REST API povolen.

“Konfigurace kontextu uživatele, který se používá pro autorizaci v produktu messaging REST API” na stránce 809
V 9.3.2 Můžete nakonfigurovat, jaký uživatelský kontext se používá pro autorizaci, když používáte produkt messaging REST API k odeslání, přijetí, procházení nebo publikování zprávy. To znamená, že můžete zvolit, zda se pro autorizaci použije uživatel, který je přihlášen k serveru messaging REST API, nebo uživatel, který spustil server mqweb.

“Konfigurace režimu připojení pro messaging REST API” na stránce 808
Produkt messaging REST API můžete nakonfigurovat tak, aby se připojoval k lokálním nebo vzdáleným správcům front.

V 9.3.3 Konfigurace režimu připojení pro messaging REST API

Produkt messaging REST API můžete nakonfigurovat tak, aby se připojoval k lokálním nebo vzdáleným správcům front.

Než začnete

Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , nelze tuto úlohu použít. Samostatný produkt IBM MQ Web Server podporuje připojení pouze ke vzdáleným správcům front.

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Informace o této úloze

Výchozí režim připojení pro messaging REST API se liší v závislosti na typu instalace, která spouští server mqweb:

- V instalaci systému IBM MQ se standardně produkt messaging REST API připojuje pouze k lokálním správcům front ve stejné instalaci jako server mqweb. Chcete-li zobrazit a změnit konfiguraci připojení, postupujte podle pokynů v této úloze.
- V 9.3.5 Linux V samostatné instalaci produktu IBM MQ Web Server produkt messaging REST API podporuje připojení pouze ke vzdáleným správcům front. Konfiguraci připojení nelze zobrazit nebo změnit.

Procedura

- Zobrazte aktuální konfiguraci serveru messaging REST API pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestMessagingConnectionMode` zobrazuje aktuální režim připojení. Pokud je hodnota `local`, může se agent messaging REST API připojit pouze ke správcům front ve stejné instalaci jako server mqweb. Je-li hodnota `remote`, může se agent messaging REST API připojit ke vzdáleným správcům front.
- Nakonfigurujte server mqweb tak, aby umožňoval serveru messaging REST API připojení pouze ke správcům front, kteří jsou ve stejné instalaci jako server mqweb, pomocí následujících příkazů:

  ```
  setmqweb properties -k mqRestMessagingConnectionMode -v local
  endmqweb
  strmqweb
  ```
- Nakonfigurujte server mqweb tak, aby umožňoval serveru messaging REST API připojení ke vzdáleným správcům front pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingConnectionMode -v remote
  endmqweb
  strmqweb
  ```

Jak pokračovat dále

Pokud nakonfigurujete server mqweb tak, aby umožňoval serveru messaging REST API připojení ke vzdáleným správcům front, musíte poskytnout informace o připojení pro každého správce front, ke kterému se chcete připojit. Další informace o způsobu poskytování informací o připojení naleznete v tématu Nastavení vzdáleného správce front pro použití s produktem messaging REST API.

Související úlohy

“Povolení messaging REST API” na stránce 805
Můžete nakonfigurovat, zda je messaging REST API povolen, pomocí příkazu **setmqweb** . Standardně je messaging REST API povolen.

“Konfigurace sdružování připojení pro messaging REST API” na stránce 806
Můžete nakonfigurovat maximální počet připojení ve fondu, která mohou být použita produktem messaging REST API, a chování agenta messaging REST API , když jsou všechna připojení používána.

“Konfigurace kontextu uživatele, který se používá pro autorizaci v produktu messaging REST API” na stránce 809
V 9.3.2 Můžete nakonfigurovat, jaký uživatelský kontext se používá pro autorizaci, když používáte produkt messaging REST API k odeslání, přijetí, procházení nebo publikování zprávy. To znamená, že můžete zvolit, zda se pro autorizaci použije uživatel, který je přihlášen k serveru messaging REST API, nebo uživatel, který spustil server mqweb.

V 9.3.2 Konfigurace kontextu uživatele, který se používá pro autorizaci v produktu messaging REST API

V 9.3.2 Můžete nakonfigurovat, jaký uživatelský kontext se používá pro autorizaci, když používáte produkt messaging REST API k odeslání, přijetí, procházení nebo publikování zprávy. To znamená, že můžete zvolit, zda se pro autorizaci použije uživatel, který je přihlášen k serveru messaging REST API, nebo uživatel, který spustil server mqweb.

Než začnete

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.
- Linux V 9.3.5 Pokud je server mqweb součástí samostatné instalace produktu IBM MQ Web Server , musíte mít přístup pro zápis k souboru `mqwebuser.xml` v datovém adresáři IBM MQ Web Server .

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Informace o této úloze

- Když je použité ID uživatele ID uživatele, které je přihlášeno k produktu messaging REST API, je hodnota **MQMD.UserIdentifier** nastavena na ID uživatele, které je přihlášeno k rozhraní REST API. Parametr **MQMD.AppIdentityData** je nastaven na ID uživatele, který je přihlášen k rozhraní REST API.
- Je-li použité ID uživatele ID uživatele, který spustil server mqweb, ponechá pole **MQMD.UserIdentifier** prázdné. Parametr **MQMD.AppIdentityData** je nastaven na ID uživatele, který je přihlášen k rozhraní REST API.

Další informace o částech deskriptoru zpráv zprávy IBM MQ naleznete v tématu MQMD .

Procedura

- Zobrazte aktuální konfiguraci serveru messaging REST API pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestMessagingAdoptWebUserContext` zobrazuje, jaké ID uživatele se používá pro autorizaci, když odesíláte, publikujete, přijímáte nebo procházíte zprávy. Pokud je hodnota `True`, uživatel, který je přihlášen k serveru messaging REST API , se použije pro autorizaci. Pokud je hodnota `False` , použije se pro autorizaci uživatel, který spustil server mqweb.
- Nakonfigurujte produkt messaging REST API tak, aby používal ID uživatele, který je přihlášen k produktu messaging REST API pro autorizaci, pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingAdoptWebUserContext -v true
  ```

  Když je parametr **mqRestMessagingAdoptWebUserContext** nastaven na hodnotu `true`, je parametr **MQMD.UserIdentifier** nastaven na ID uživatele, který je přihlášen k rozhraní REST API. Parametr **MQMD.AppIdentityData** je nastaven na ID uživatele, který je přihlášen k rozhraní REST API.
- Nakonfigurujte messaging REST API tak, aby používal ID uživatele, který spustil server mqweb, pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingAdoptWebUserContext -v false
  ```

Je-li parametr **mqRestMessagingAdoptWebUserContext** nastaven na hodnotu `false`, pole **MQMD.UserIdentifier** zůstane prázdné. Parametr **MQMD.AppIdentityData** je nastaven na ID uživatele, který je přihlášen k rozhraní REST API.

Související úlohy

“Povolení messaging REST API” na stránce 805
Můžete nakonfigurovat, zda je messaging REST API povolen, pomocí příkazu **setmqweb** . Standardně je messaging REST API povolen.

“Konfigurace sdružování připojení pro messaging REST API” na stránce 806
Můžete nakonfigurovat maximální počet připojení ve fondu, která mohou být použita produktem messaging REST API, a chování agenta messaging REST API , když jsou všechna připojení používána.

“Konfigurace režimu připojení pro messaging REST API” na stránce 808
Produkt messaging REST API můžete nakonfigurovat tak, aby se připojoval k lokálním nebo vzdáleným správcům front.

Konfigurace REST API pro MFT

Standardně není REST API pro MFT povoleno. Můžete konfigurovat, zda je povolena funkce REST API for MFT , nastavit koordinačního správce front, nastavit správce front příkazů a zadat časový limit opětovného připojení MFT pomocí příkazu **setmqweb properties** .

Procedura

- “Povolení REST API pro MFT” na stránce 811
- “Konfigurace koordinačního správce front pro REST API pro MFT” na stránce 812
- “Konfigurace správce front příkazů pro REST API pro MFT” na stránce 813
- “Konfigurace REST API pro hodnoty časového limitu MFT” na stránce 814

Povolení REST API pro MFT

Než budete moci použít REST API pro MFT, musíte nejprve povolit REST API pro MFT. Můžete nakonfigurovat, zda je REST API for MFT povolen, pomocí příkazu **setmqweb** . Standardně není REST API pro MFT povoleno.

Než začnete

Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , nelze tuto úlohu použít. REST API for MFT není k dispozici v samostatné instalaci produktu IBM MQ Web Server .

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do crtmqweb. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Postup

1. Zobrazte aktuální konfiguraci REST API pro MFT pomocí následujícího příkazu:

   ```
   dspmqweb properties -a
   ```

   Pole mqRestMftEnabled zobrazuje, zda je povolena volba REST API for MFT . Hodnota je True , pokud je REST API pro MFT povoleno, nebo False jinak.
2. Povolte nebo zakažte REST API pro MFT pomocí jednoho z následujících příkazů:
   - Povolte REST API pro MFT pomocí následujícího příkazu:

     ```
     setmqweb properties -k mqRestMftEnabled -v true
     ```
   - Zakažte REST API pro MFT pomocí následujícího příkazu:

     ```
     setmqweb properties -k mqRestMftEnabled -v false
     ```
3. Restartujte server mqweb zadáním následujících příkazů:

   ```
   endmqweb
   strmqweb
   ```

Jak pokračovat dále

Pokud jste povolili REST API pro MFT, musíte nastavit název koordinačního správce front, než budete moci použít REST API pro MFT. Další informace o nastavení koordinačního správce front viz “Konfigurace koordinačního správce front pro REST API pro MFT” na stránce 812.

Konfigurace koordinačního správce front pro REST API pro MFT

Než budete moci použít REST API pro MFT, musíte nakonfigurovat správce front tak, aby fungoval jako koordinační správce front pro transakce MFT . Můžete nastavit, který správce front je koordinačním správcem front, pomocí příkazu **setmqweb** .

Než začnete

Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , nelze tuto úlohu použít. REST API for MFT není k dispozici v samostatné instalaci produktu IBM MQ Web Server .

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru mqwebuser.xml .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do crtmqweb. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Postup

1. Zobrazte aktuální konfiguraci REST API pro MFT pomocí následujícího příkazu:

   ```
   dspmqweb properties -a
   ```

   V poli mqRestMftCoordinationQmgr je uveden název koordinačního správce front.
2. Konfigurujte koordinačního správce front pomocí následujícího příkazu:

   ```
   setmqweb properties -k mqRestMftCoordinationQmgr -v qmgrName
   ```

   kde *qmgrName* je název koordinačního správce front. Koordinační správce front musí být na počítači, na kterém je spuštěn server mqweb. Standardně je tento název správce front prázdný. Není-li hodnota nastavena, REST API pro MFT nefunguje.
3. Restartujte server mqweb zadáním následujících příkazů:

   ```
   endmqweb
   strmqweb
   ```

Jak pokračovat dále

- Ujistěte se, že je REST API pro MFT povoleno. Další informace viz téma “Povolení REST API pro MFT” na stránce 811.
- Chcete-li použít REST API pro MFT k odeslání požadavků na vytvoření, musíte nastavit název správce front příkazů. Chcete-li například použít příkaz REST API , například **create transfer**, musíte nastavit název správce front příkazů. Další informace viz “Konfigurace správce front příkazů pro REST API pro MFT” na stránce 813.
- Můžete nakonfigurovat REST API pro hodnoty časového limitu MFT . Výchozí časový limit je 30 minut. Další informace viz téma “Konfigurace REST API pro hodnoty časového limitu MFT” na stránce 814.
- Chcete-li použít REST API pro MFT, musí být uživatel ověřen na serveru mqweb a musí být členem jedné nebo více rolí MFTWebAdminnebo MFTWebAdminRO . Další informace o konfiguraci uživatelů naleznete v tématu Konfigurace uživatelů a rolí pro produkt REST API.

Konfigurace správce front příkazů pro REST API pro MFT

Než budete moci použít REST API pro MFT k odeslání požadavků na vytvoření, musíte nastavit název správce front příkazů. Chcete-li například použít prostředek **create transfer** , musíte nastavit název správce front příkazů. Název správce front příkazů můžete nastavit pomocí příkazu **setmqweb** .

Než začnete

Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , nelze tuto úlohu použít. REST API for MFT není k dispozici v samostatné instalaci produktu IBM MQ Web Server .

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru mqwebuser.xml .

- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Postup

1. Zobrazte aktuální konfiguraci REST API pro MFT pomocí následujícího příkazu:

   ```
   dspmqweb properties -a
   ```

   V poli `mqRestMftCommandQmgr` je uveden název správce front příkazů.
2. Konfigurujte správce front příkazů pomocí následujícího příkazu:

   ```
   setmqweb properties -k mqRestMftCommandQmgr -v qmgrName
   ```

   kde *qmgrName* je název správce front příkazů. Správce front příkazů musí být v počítači, kde je spuštěn server mqweb. Standardně je tento název správce front prázdný. Není-li hodnota nastavena, REST API pro MFT pro příkaz k vytvoření nefunguje.
3. Restartujte server mqweb zadáním následujících příkazů:

   ```
   endmqweb
   strmqweb
   ```

Jak pokračovat dále

- Ujistěte se, že je REST API pro MFT povoleno. Další informace viz téma “Povolení REST API pro MFT” na stránce 811.
- Ujistěte se, že je nastaven koordinační správce front. Další informace viz téma “Konfigurace koordinačního správce front pro REST API pro MFT” na stránce 812.
- Můžete nakonfigurovat REST API pro hodnoty časového limitu MFT . Výchozí časový limit je 30 minut. Další informace viz téma “Konfigurace REST API pro hodnoty časového limitu MFT” na stránce 814.
- Chcete-li použít REST API pro MFT, musí být uživatel ověřen na serveru mqweb a musí být členem jedné nebo více rolí `MFTWebAdmin`nebo `MFTWebAdminRO` . Další informace o konfiguraci uživatelů naleznete v tématu Konfigurace uživatelů a rolí pro produkt REST API.

Konfigurace REST API pro hodnoty časového limitu MFT

Můžete konfigurovat dobu v minutách, po jejímž uplynutí se konzola REST API for MFT přestane pokoušet o připojení ke koordinačnímu správci front po přerušení připojení. Výchozí časový limit je 30 minut. Tento časový limit můžete nakonfigurovat pomocí příkazu **setmqweb** .

Než začnete

Poznámka: V 9.3.5 Linux Pokud je server mqweb spuštěn v samostatné instalaci produktu IBM MQ Web Server , nelze tuto úlohu použít. REST API for MFT není k dispozici v samostatné instalaci produktu IBM MQ Web Server .

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSmusíte mít oprávnění ke spuštění příkazů **dspmqweb** a **setmqweb** a k zápisu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: z/OS

Před zadáním příkazů **setmqweb** nebo **dspmqweb** v systému z/OSmusíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby ukazovala na konfiguraci serveru mqweb.

Chcete-li nastavit proměnnou prostředí WLP_USER_DIR, zadejte následující příkaz:

```
export WLP_USER_DIR=WLP_user_directory
```

kde *WLP_user_directory* je název adresáře, který je předán do `crtmqweb`. Příklad:

```
export WLP_USER_DIR=/var/mqm/web/installation1
```

Další informace viz téma Vytvoření serveru mqweb.

Informace o této úloze

Můžete nakonfigurovat časový limit pro REST API pro MFT.

Agent REST API for MFT se pokusí znovu navázat připojení ihned po přerušení připojení ke koordinačnímu správci front. Pokud se tento pokus nezdaří, je mezi každým pokusem o opětovné připojení interval pěti minut, dokud časový limit neuplyne. Proto nastavení hodnoty mezi 0-5 má za následek pouze jeden pokus o opětovné připojení.

Po vypršení časového limitu opětovného připojení se další pokus o opětovné připojení provede při vyvolání kteréhokoli z prostředků REST API for MFT . Pokud se tento pokus o opětovné připojení nezdaří, produkt MFT se znovu pokusí znovu připojit každých pět minut, dokud neuplyne časový limit pro opětovné připojení.

Postup

1. Zobrazte aktuální konfiguraci REST API pro MFT pomocí následujícího příkazu:

   ```
   dspmqweb properties -a
   ```

   Pole `mqRestMftReconnectTimeoutInMinutes` zobrazuje hodnotu časového limitu opětovného připojení, dokud se služby MFT Transfer Rest nezastaví při pokusu o připojení ke koordinačnímu správci front.
2. Nakonfigurujte časový limit v minutách, po jehož uplynutí se konzola REST API for MFT přestane pokoušet o připojení ke koordinačnímu správci front:
   - Resetovat časový limit na výchozí hodnotu 30 minut:

     ```
     setmqweb properties -k mqRestMftReconnectTimeoutInMinutes -d
     ```
   - Nastavit časový limit:

     ```
     setmqweb properties -k mqRestMftReconnectTimeoutInMinutes -v time
     ```

kde *čas* uvádí čas v minutách, než dojde k vypršení časového limitu.

Je-li tato hodnota nastavena mezi `0-5`, REST API for MFT se pokusí znovu připojit ke koordinačnímu správci front pouze jednou. Pokud připojení selže, nedojde k žádným pokusům o opětovné vytvoření připojení, dokud nebude vyvolán REST API .

Pokud je tato hodnota nastavena na `-1`, REST API for MFT se pokusí znovu připojit, dokud nebude připojení úspěšné.

3. Restartujte server mqweb zadáním následujících příkazů:

```
endmqweb
strmqweb
```

Jak pokračovat dále

- Ujistěte se, že je REST API pro MFT povoleno. Další informace viz téma “Povolení REST API pro MFT” na stránce 811.
- Ujistěte se, že je nastaven koordinační správce front. Další informace viz téma “Konfigurace koordinačního správce front pro REST API pro MFT” na stránce 812.
- Chcete-li použít REST API pro MFT k odeslání požadavků na vytvoření, musíte nastavit název správce front příkazů. Chcete-li například použít příkaz REST API , například **`create transfer`**, musíte nastavit název správce front příkazů. Další informace viz “Konfigurace správce front příkazů pro REST API pro MFT” na stránce 813.
- Chcete-li použít REST API pro MFT, musí být uživatel ověřen na serveru mqweb a musí být členem jedné nebo více rolí `MFTWebAdmin`nebo `MFTWebAdminRO` . Další informace o konfiguraci uživatelů naleznete v tématu Konfigurace uživatelů a rolí pro produkt REST API.

Vyladění prostředí JVM serveru mqweb

Standardně používá prostředí JVM (mqweb server Java Virtual Machine) výchozí nastavení specifické pro platformu pro konfigurační parametry, jako je minimální a maximální velikost haldy a velikost mezipaměti tříd.

Informace o této úloze

Možná budete muset změnit výchozí hodnoty, abyste zlepšili výkon nebo vyřešili problémy. Pokud například server mqweb vygeneruje `java.lang.OutOfMemoryError` , musíte zvýšit maximální velikost haldy. Pokud se pokoušíte načíst velký počet objektů fronty, měli byste také zvýšit velikost haldy.

Pokud máte problémy se zobrazením informací o konfiguraci řídicího panelu v produktu IBM MQ Console, musíte nastavit proměnnou, která určuje kódování souboru konfigurace. Výchozí hodnoty můžete změnit v souboru `jvm.options` .

Postup

1. Otevřete soubor `jvm.options` .

   Soubor `jvm.options` lze nalézt v jednom z následujících adresářů:

   - V instalaci produktu IBM MQ :
     - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*`installationName`*`/servers/mqweb`
     - Windows V systému Windows: *`MQ_DATA_PATH`*`\web\installations\`*`installationName`*`\servers\mqweb`, kde *`MQ_DATA_PATH`* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
     - IBM i V systému IBM i: *`MQ_DATA_PATH`*`/web/installations/Installation1/`

– z/OS V systému z/OS: *WLP_user_directory*/servers/mqweb

kde *WLP_user_directory* je adresář určený při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.

- V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*/web/installations/MQWEBINST/servers/mqweb

  kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

2. Volitelné: Nastavte maximální velikost haldy přidáním následujícího řádku do souboru:

```
-Xmx<i>MaxSize</i>m
```

   Kde *MaxSize* uvádí maximální velikost haldy v MB.

   Například následující řádek nastaví maximální velikost haldy na 1GB:

```
-Xmx1024m
```

3. Volitelné: Nastavte minimální velikost haldy přidáním následujícího řádku do souboru:

```
-Xms<i>MinSize</i>m
```

   Kde *MinSize* uvádí minimální velikost haldy v MB. Zvýšení minimální velikosti haldy z výchozího nastavení může snížit dobu potřebnou ke spuštění serveru mqweb.

   Například následující řádek nastaví minimální velikost haldy na 512MB:

```
-Xms512m
```

4. Volitelné: Nastavte velikost mezipaměti tříd přidáním následujícího řádku do souboru:

```
-Xscmx<i>Size</i>m
```

   Kde *Velikost* uvádí velikost mezipaměti třídy, v MB.

   Například následující řádek nastaví velikost mezipaměti třídy na 100MB:

```
-Xscmx100m
```

   Mezipaměť sdílených tříd Java se používá k ukládání dat, jako jsou například načtené třídy a kompilovaný kód AOT (Ahead-of-Time).

   Mezipaměť tříd výrazně zkracuje dobu potřebnou ke spuštění serveru mqweb. Při prvním spuštění serveru mqweb je vytvořena mezipaměť tříd a spuštění serveru může trvat delší dobu. Následná restartování serveru budou mnohem rychlejší, protože třídy lze načíst z mezipaměti sdílených tříd.

   Zvýšení velikosti mezipaměti tříd z výchozího nastavení může snížit dobu potřebnou ke spuštění serveru mqweb.

   z/OS Mezipaměť tříd je znovu vytvořena, když je server mqweb spuštěn na jiném systému z/OS . Proto spuštění serveru mqweb v jiném systému z/OS v prostředí sysplex může trvat podstatně déle než restartování serveru ve stejném systému.

   Všimněte si, že změny této hodnoty se projeví pouze při vytvoření mezipaměti tříd. Mezipaměť tříd je vytvořena při prvním spuštění serveru mqweb nebo po zničení mezipaměti tříd pomocí obslužného programu mezipaměti tříd Java .

5. Požadované: Zkontrolujte, zda soubor obsahuje následující řádky pro uvedení kódování souboru, které se použije, když REST API zpracovává data, a pro informace o konfiguraci uživatelského panelu dashboard v souboru IBM MQ Console:

```
-Dfile.encoding=UTF-8
-Ddefault.client.encoding=UTF-8
```

6. Restartujte server mqweb.

z/OS V systému z/OSzastavte a restartujte spuštěnou úlohu serveru mqweb.

Multi Na všech ostatních platformách zadejte na příkazový řádek následující příkazy:

```
endmqweb
strmqweb
```

Struktura souboru komponenty instalace IBM MQ Console a REST API

Existují dvě sady adresářových struktur, které jsou přidruženy k instalačním komponentám IBM MQ Console a REST API . Jedna adresářová struktura obsahuje soubory, které lze upravovat. Ostatní adresářová struktura obsahuje soubory, které nelze upravit.

Upravitelné soubory

Uživatelem upravitelné soubory jsou stanoveny jako součást počáteční instalace komponent instalace IBM MQ Console a REST API . Vzhledem k tomu, že tyto soubory lze upravovat, soubory se při použití údržby nezmění.

Umístění uživatelsky upravitelných souborů závisí na operačním systému a nainstalovaném produktu.

- V instalaci produktu IBM MQ jsou uživatelem upravitelné soubory v jednom z následujících adresářů:
  - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*`installationName`*
  - Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
  - z/OS V systému z/OS: adresář, který byl zadán při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.
- V 9.3.5 Linux V samostatné IBM MQ Web Server instalaci: *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST`

  kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

V tomto adresáři nejvyšší úrovně jsou přítomny následující adresáře a soubory:

Adresáře a soubory	Popis
`angular.persistence/`	Adresář, kde je uložena konfigurace řídicího panelu IBM MQ Console .
`servers/`	Adresář serverů WebSphere Liberty .
`servers/mqweb`	Adresář, který obsahuje adresářovou strukturu serveru mqweb.
`servers/mqweb/logs`	Adresář, který obsahuje protokoly pro server mqweb.
`servers/mqweb/logs/console.log`	Protokol základních zpráv o stavu serveru a provozu.
`servers/mqweb/logs/ffdc`	Výstupní adresář FFDC (First Failure Data Capture).
`servers/mqweb/logs/messages.log`	Protokol běhových zpráv ze serveru mqweb, včetně IBM MQ Console a REST API. Starší zprávy jsou uloženy v souborech s názvem `messages_`*`timestamp`*`.log`.

Adresáře a soubory	Popis
`servers/mqweb/logs/trace.log`	Protokol trasování ze serveru mqweb, včetně protokolů IBM MQ Console a REST API. Starší trasování je uloženo v souborech s názvem `trace_`*`timestamp`*`.log`. Tyto soubory existují pouze v případě, že je povoleno trasování.
`servers/mqweb/logs/state`	Stav specifický pro server.
`servers/mqweb/server.xml`	Hlavní konfigurační soubor serveru. Tento soubor je jen pro čtení. Upravte soubor `mqwebuser.xml` a přepište výchozí konfiguraci.
`servers/mqweb/mqwebuser.xml`	Konfigurační soubor pro IBM MQ Console a REST API. Nastavení, která jsou nakonfigurována v tomto souboru, přepíší výchozí konfiguraci. Chcete-li tento soubor upravit, musíte být privilegovaný uživatel .
`servers/mqweb/resources`	Adresář, který obsahuje různé prostředky serveru, například úložiště klíčů.
`servers/mqweb/workarea`	Adresář, který je vytvořen serverem při jeho provozu. Tento adresář je vytvořen po prvním spuštění serveru.

Neupravitelné soubory

Neupravitelné soubory jsou stanoveny jako součást počáteční instalace komponent instalace IBM MQ Console a REST API . Tyto soubory jsou aktualizovány při použití údržby.

Umístění neupravitelných souborů závisí na operačním systému a nainstalovaném produktu.

- V instalaci produktu IBM MQ jsou neupravitelné soubory v jednom z následujících adresářů:
  - ALW V systému AIX, Linux, and Windows: *MQ_INSTALLATION_PATH*`/web`
  - IBM i V systému IBM i: *MQ_INSTALLATION_PATH*`/web`
  - z/OS V systému z/OS: *`installation_directory`*`/web/`

    kde *instalační_adresář* je instalační cesta IBM MQ for z/OS UNIX System Services Components .
- V 9.3.5 Linux V samostatné instalaci produktu IBM MQ Web Server se jedná o adresář, do kterého byl dekomprimován instalační soubor IBM MQ Web Server .

V tomto umístění se nachází následující adresářová struktura a soubory:

Adresáře a soubory	Popis
`bin/`	Adresář, který obsahuje příkazy WebSphere Liberty . Chcete-li spouštět skripty v tomto adresáři, musíte být privilegovaný uživatel .
`mq/`	Adresářová struktura, která obsahuje různé prostředky IBM MQ .
`mq/apps/`	Adresář, který obsahuje aplikace IBM MQ Console a REST API .

Adresáře a soubory	Popis
`mq/etc/`	
`mq/etc/mqweb.xml`	Konfigurační soubor jen pro čtení pro server mqweb. Upravte soubor `mqwebuser.xml` a proveďte změny konfigurace.
`mq/libs`	Adresář, který obsahuje sdílené knihovny pro použití v adresářích IBM MQ Console a REST API.
`mq/samp`	Adresář, který obsahuje ukázky.
`mq/samp/configuration`	Adresář, který obsahuje ukázkové konfigurační soubory, které lze zkopírovat do souboru `mqwebuser.xml` .

Zálohování a obnova konfigurace serveru mqweb

Můžete zálohovat konfiguraci serveru mqweb a obnovit ji do stejného umístění nebo do jiného umístění.

Než začnete

Než budete moci obnovit konfiguraci serveru mqweb, musíte nainstalovat produkt IBM MQnebo samostatný IBM MQ Web Server, na systém, kde chcete obnovit server mqweb. V samostatné instalaci produktu IBM MQ Web Server musíte vytvořit server mqweb podle kroků v části “Konfigurace samostatného serveru IBM MQ Web Server” na stránce 790.

Informace o této úloze

Chcete-li zálohovat a obnovit konfiguraci serveru mqweb, postupujte podle pokynů v této úloze. Pokud obnovíte server mqweb do jiného umístění, musíte aktualizovat konfiguraci serveru mqweb, abyste se ujistili, že odkazy na soubory jsou správné.

V 9.3.5 Tento postup můžete také použít k migraci serveru mqweb, který je aktuálně spuštěn v instalaci produktu IBM MQ , aby se spustil v samostatné instalaci produktu IBM MQ Web Server .

Postup

1. Chcete-li zálohovat konfiguraci serveru mqweb, zkopírujte všechny soubory v adresáři, který obsahuje konfiguraci serveru mqweb, do umístění zálohy.
   - V instalaci produktu IBM MQ zkopírujte obsah následujícího adresáře:
     - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/`*`installationName`*
     - Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
     - z/OS V systému z/OS: uživatelský adresář WebSphere Liberty , který byl zadán při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.
   - V 9.3.5 Linux V samostatné instalaci produktu IBM MQ Web Server zkopírujte obsah adresáře *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST` , kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který odkazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .

2. Chcete-li obnovit konfiguraci serveru mqweb, nahraďte obsah adresáře, který obsahuje konfiguraci serveru mqweb, soubory, které jste zkopírovali v kroku “1” na stránce 820.
   - V instalaci produktu IBM MQ nahraďte obsah následujícího adresáře:
     - Linux AIX V systému AIX nebo Linux: `/var/mqm/web/installations/installationName`
     - Windows V systému Windows: *MQ_DATA_PATH*`\web\installations\`*installationName*, kde *MQ_DATA_PATH* je cesta k datům IBM MQ . Tato cesta je cestou k datům, která je vybrána během instalace produktu IBM MQ. Standardně je tato cesta `C:\ProgramData\IBM\MQ`.
     - z/OS V systému z/OS: uživatelský adresář WebSphere Liberty , který byl zadán při spuštění skriptu **crtmqweb** za účelem vytvoření definice serveru mqweb.
   - V 9.3.5 Linux V samostatné instalaci produktu IBM MQ Web Server nahraďte obsah adresáře *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST` , kde *MQ_OVERRIDE_DATA_PATH* je datový adresář IBM MQ Web Server , na který ukazuje proměnná prostředí **MQ_OVERRIDE_DATA_PATH** .
3. Nastavte vlastnictví souborů, které jste obnovili v kroku “2” na stránce 821 , aby ID uživatele serveru mqweb mohlo k souborům přistupovat.
4. Pokud jste obnovili konfiguraci serveru mqweb do jiného umístění, změňte hodnotu všech vlastností v konfiguraci serveru mqweb, které odkazují na soubory v předchozím konfiguračním adresáři serveru mqweb.
   a) Před zadáním příkazů **setmqweb** nebo **dspmqweb** nastavte prostředí tak, aby ukazovaly na konfiguraci serveru mqweb.
      - z/OS V systému z/OSnastavte proměnnou prostředí **WLP_USER_DIR** tak, aby ukazovala na konfiguraci serveru mqweb, zadáním následujícího příkazu:

        ```
        export WLP_USER_DIR=WLP_user_directory
        ```

        kde *WLP_user_directory* je název adresáře, který je předán příkazu **crtmqweb** .

        Další informace viz téma Vytvoření serveru mqweb.
      - V 9.3.5 Linux V samostatné instalaci produktu IBM MQ Web Server nastavte proměnnou prostředí **MQ_OVERRIDE_DATA_PATH** na datový adresář IBM MQ Web Server .
      - Ve všech ostatních prostředích nemusíte provádět žádné akce pro nastavení prostředí.

   b) Zobrazte hodnotu všech konfigurovatelných vlastností serveru mqweb, které uživatel upravil. Spusťte následující příkaz:

      ```
      dspmqweb properties -u
      ```

   c) Pokud se zobrazí vlastnost **remoteKeyfile** , zkontrolujte hodnotu vlastnosti.

      Pokud hodnota vlastnosti odkazuje na cestu k souboru v předchozím konfiguračním adresáři serveru mqweb, změňte hodnotu tak, aby odkazovala na cestu k souboru v novém konfiguračním adresáři serveru mqweb. Chcete-li změnit hodnotu vlastnosti **remoteKeyfile** , zadejte následující příkaz:

      ```
      setmqweb properties -k remoteKeyfile -v path_to_keyfile
      ```

   d) Zobrazte konfiguraci vzdáleného správce front serveru mqweb. Spusťte následující příkaz:

      ```
      dspmqweb remote -a
      ```

   e) Pokud se zobrazí některá z následujících vlastností, zkontrolujte hodnotu vlastnosti:
      - **globalTrustStorePath**

- **globalKeyStorePath**
- **ccdtURL**
- **keyStorePath**
- **trustStorePath**

Změňte hodnotu vlastnosti odkazující na cestu k souboru v předchozím konfiguračním adresáři serveru mqweb tak, aby odkazovala na cestu k souboru v novém konfiguračním adresáři serveru mqweb. Zadáním příkazu **setmqweb remote** změňte hodnotu každé vlastnosti. Chcete-li například změnit hodnotu vlastnosti **keyStorePath** pro vzdáleného správce front s jedinečným názvem `remote-QM1`, zadejte následující příkaz:

```
setmqweb remote -uniqueName remote-QM1 -keyStorePath new_keystore_path
```

Další informace viz setmqweb remote (set mqweb server remote queue manager configuration).

Windows Linux MQ Adv. MQ Adv. VUE MQ Adv. z/OS Definování připojení Aspera gateway na platformách Linux nebo Windows

Produkt IBM Aspera faspio Gateway poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě IBM MQ. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows.

Informace o této úloze

Produkt Aspera gateway lze použít ke zlepšení výkonu kanálů správce front. Je zvláště efektivní, pokud má síť vysokou latenci nebo má tendenci ztrácet pakety, a obvykle se používá k urychlení připojení mezi správci front v různých datových střediscích.

Poznámka: Pro rychlou síť, která neztrácí pakety, dochází ke snížení výkonu při použití Aspera gateway, takže je důležité zkontrolovat výkon sítě před a po definování připojení Aspera gateway .

Na každém konci síťového připojení IP definujete Aspera gateway a poté pomocí protokolu TCP/IP připojíte kanály správce front ke každé bráně. Správce front nemusí být spuštěn ve stejném počítači jako server Aspera gateway , který používá, a více správců front může používat stejnou bránu.

Chcete-li použít produkt Aspera gateway, musíte mít jeden nebo více z následujících nároků:

- IBM MQ Advanced for Multiplatforms
- IBM MQ Appliance
- IBM MQ Advanced for z/OS VUE
- LTS V 9.3.4 IBM MQ Advanced for z/OS, buď Long Term Support , nebo Continuous Delivery z IBM MQ 9.3.4

Produkt Aspera gateway můžete implementovat na libovolné z následujících platforem:

- Linux for x86-64
- Linux on Power Systems - Little Endian
- Linux for IBM Z
- Windows -další informace o podpoře platformy v systému Windowsnaleznete v IBM Aspera faspio Gateway dokumentaci.

Použití Aspera gateway je omezeno na zprávy IBM MQ , pokud není brána samostatně oprávněna.

Správci front, kteří používají produkt Aspera gateway , mohou být spuštěni na libovolné podporované platformě. Úplný seznam podporovaných platforem naleznete v tématu Ikony použité v dokumentaci k produktu.

U každého správce front, který není ve stejném počítači jako správce front Aspera gateway , který používá, zkontrolujte, zda máte rychlé síťové připojení mezi správcem front a správcem front Aspera gateway.

Pomocí souboru `toml` vytvoříte definici brány, která definuje příchozí a odchozí porty, které brána používá. Ukázkový soubor `toml` se dodává s produktem Aspera gateway. Definice odchozí brány definuje připojení z lokálního správce front k bráně a z lokální brány ke vzdálené bráně. Definice příchozí brány definuje připojení ze vzdálené brány k lokální bráně a z lokální brány k lokálnímu správci front.

Následující kroky poskytují základní vodítko pro spuštění a spuštění. Podrobnější informace naleznete v IBM Aspera faspio Gateway dokumentaci.

Postup

1. Získejte obraz instalace Aspera gateway .

   Multi V případě platformy Multiplatforms stáhnete soubor Aspera gateway z webu Passport Advantage. Soubor ke stažení je označen "IBM Aspera faspio Continuous Delivery Release for IBM MQ V9.3 Multiplatform Multilingual eAssembly". Dodává se jako obraz Continuous Delivery (CD) pouze kvůli tempu změn v této oblasti, což znamená, že jsou potřebné aktualizace na frekvenci vydání CD a můžete je nainstalovat na libovolný systém IBM MQ , který má nárok IBM MQ Advanced for Multiplatforms nebo IBM MQ Appliance . Chcete-li stáhnout toto eAssembly, přejděte na Stahování IBM MQ 9.3 a poté klepněte na kartu pro požadované vydání. eAssembly obsahuje obrazy instalace pro všechny platformy, na kterých je brána k dispozici. V 9.3.0 V 9.3.0 eAssembly také obsahuje soubor `ibm-faspio-license.zip` , který obsahuje soubor s licencemi.

   LTS V 9.3.4 MQ Adv. VUE MQ Adv. z/OS Pokud má váš systém IBM MQ nárok IBM MQ Advanced for z/OS VUE nebo nárok IBM MQ Advanced for z/OS , buď Long Term Support, nebo Continuous Delivery z IBM MQ 9.3.4, získáte Aspera gateway z komponenty Connector Pack, která je součástí instalace SMP/E.

   MQ Adv. VUE MQ Adv. z/OS Soubory pro IBM MQ Advanced for z/OS VUE a IBM MQ Advanced for z/OS jsou následující:

Tabulka 52. Názvy souborů a čísla verzí faspio podle platformy a verze IBM MQ

Platforma	Název souboru	Číslo verze faspio
Linux for x86-64	V 9.3.4 `M0C5LEN.zip`	1.3.3
Linux on Power Systems - Little Endian	V 9.3.4 `M0C5MEN.zip`	1.3.3
Linux for IBM Z	V 9.3.4 `M0C5NEN.zip`	1.3.3
Windows	V 9.3.4 `M0C5PEN.zip`	1.3.3
Linux for x86-64	V 9.3.3 `M0B2XEN.zip`	1.3.2
Linux on Power Systems - Little Endian	V 9.3.3 `M0B2YEN.zip`	1.3.2
Linux for IBM Z	V 9.3.3 `M0B2ZEN.zip`	1.3.2
Windows	V 9.3.3 `M0B30EN.zip`	1.3.2
Linux for x86-64	V 9.3.2 `M090HEN.zip`	1.3.1

Tabulka 52. Názvy souborů a čísla verzí faspio podle platformy a verze IBM MQ (pokračování)		
Platforma	**Název souboru**	**Číslo verze faspio**
Linux on Power Systems - Little Endian	V 9.3.2 M090JEN.zip	1.3.1
Linux for IBM Z	V 9.3.2 M090KEN.zip	1.3.1
Windows	V 9.3.2 M090LEN.zip	1.3.1
Linux for x86-64	V 9.3.0 M0559EN.zip	1.3.0
Linux on Power Systems - Little Endian	V 9.3.0 M055BEN.zip	1.3.0
Linux for IBM Z	V 9.3.0 M055CEN.zip	1.3.0
Windows	V 9.3.0 M055DEN.zip	1.3.0

Všimněte si, že Aspera gateway nelze spustit nativně na z/OS.

V 9.3.0 MQ Adv. VUE V 9.3.0 MQ Adv. z/OS Kromě obrazů instalace obsahuje adresář `fasp` adresář `M05QKEN.zip`, který obsahuje soubor s licencí.

2. Zkopírujte obraz instalace produktu Aspera gateway na dva počítače, na kterých bude brána spuštěna, a poté bránu extrahujte a nainstalujte.

   V 9.3.0 V 9.3.0 Použijte soubor s licencemi obsažený v adresáři `ibm-faspio-license.zip` (Multiplatforms) nebo `M05QKEN.zip` (z/OS). Další informace naleznete v dokumentaci k produktu IBM Aspera faspio Gateway :

   - Linux Instalace v systému Linux
   - Windows Instalace v systému Windows

3. Nakonfigurujte a zabezpečte každou bránu.

   V 9.3.0 V 9.3.0 Další informace naleznete v dokumentaci k produktu IBM Aspera faspio Gateway :

   - Konfigurace konfiguračního souboru brány
   - Zabezpečení brány

4. Na každém konci síťového připojení změňte definici kanálu tak, aby se připojovala k portu, na kterém lokální brána naslouchá.
5. Spusťte každou službu brány.

   V 9.3.0 V 9.3.0 Další informace naleznete v dokumentaci k produktu IBM Aspera faspio Gateway :

   - Linux Spuštění na Linux
   - Windows Spuštění na Windows

6. Restartujte kanály.

   Vaši správci front nyní komunikují v rámci připojení produktu Aspera gateway .

Příklad

Tento příklad definuje Aspera gateway připojení na dvou počítačích s operačním systémem Linux. Konfigurace je následující:

- Adresa IP lokálního počítače brány je 9.20.193.107. Adresa IP počítače vzdálené brány je 9.20.192.115.
- Lokální správce front je spuštěn na počítači s adresou IP 9.20.121.5. Vzdálený správce front je spuštěn na počítači s adresou IP 9.20.121.25. Oba správci front naslouchají na portu 1414.
- Kanál správce front v lokálním správci front je změněn tak, aby se připojil k lokálnímu serveru Aspera gateway pomocí produktu **conname** 9.20.193.107(1500). Kanál správce front ve vzdáleném správci front je změněn tak, aby se připojil ke vzdálenému serveru Aspera gateway pomocí produktu **conname** 9.20.192.115(1500).
- V 9.3.0 V 9.3.0 V produktu IBM Aspera faspio Gateway 1.2je standardně povoleno zabezpečení TLS. Chcete-li nakonfigurovat TLS s bránou, prohlédněte si téma Zabezpečení brány v dokumentaci k produktu IBM Aspera faspio Gateway .

1. Definujte připojení Aspera gateway na lokálním počítači brány:
   - Nainstalujte soubor Aspera gateway:
     - Linux V systému Linuxpoužijte následující příkaz:

       ```
       rpm -ivh ibm-faspio-gateway-<version>.x86_64.rpm
       ```
   - Upravte soubor `gateway.toml` v adresáři, který byl vytvořen instalací:

     Upravte soubor a nastavte definice lokální brány.

     ```
     [[bridge]]
         name = "Outbound"
         [bridge.local]
                protocol = "tcp"
                    host = "9.20.193.107"
                    port = 1500
         tls_enabled = false

         [bridge.forward]
                protocol = "fasp"
                    host = "9.20.192.115"
                    port = 1600
         tls_enabled = false

     [[bridge]]
         name = "Inbound"
         [bridge.local]
                protocol = "fasp"
                    host = "9.20.193.107"
                    port = 1600
         tls_enabled = false

         [bridge.forward]
                protocol = "tcp"
                    host = "9.20.121.5"
                    port = 1414
         tls_enabled = false
     ```
   - V 9.3.0 V 9.3.0 Zkopírujte soubor `aspera-license` z adresáře `ibm-faspio-license.zip` (Multiplatforms) nebo `M05QKEN.zip` (z/OS) do adresáře `/usr/local/etc/faspio/`.
2. Opakujte předchozí krok a definujte připojení Aspera gateway na počítači vzdálené brány.
   - Upravte soubor `gateway.toml` v adresáři, který byl vytvořen instalací. Upravte soubor a nastavte definice vzdálené brány:

     ```
     [[bridge]]
         name = "Outbound"
         [bridge.local]
     ```

```
            protocol = "tcp"
                host = "9.20.193.107"
                port = 1500
    tls_enabled = false

    [bridge.forward]
            protocol = "fasp"
                host = "9.20.192.115"
                port = 1600
    tls_enabled = false

[[bridge]]
    name = "Inbound"
    [bridge.local]
            protocol = "fasp"
                host = "9.20.193.107"
                port = 1600
    tls_enabled = false

    [bridge.forward]
            protocol = "tcp"
                host = "9.20.121.5"
                port = 1414
    tls_enabled = false
```

- V 9.3.0 V 9.3.0 Zkopírujte soubor `aspera-license` z adresáře `ibm-faspio-license.zip` (Multiplatforms) nebo `M05QKEN.zip` (z/OS) do adresáře `/usr/local/etc/faspio/`.

3. Na každém konci připojení změňte definici kanálu tak, aby se připojovala k portu, na kterém lokální brána naslouchá.
   - Změňte kanál správce front v lokálním správci front tak, aby se připojoval k lokálnímu serveru Aspera gateway pomocí produktu **conname** 9.20.193.107(1500).
   - Změňte kanál správce front ve vzdáleném správci front tak, aby se připojoval ke vzdálenému systému Aspera gateway pomocí produktu **conname** 9.20.192.115(1500).
4. Spusťte lokální bránu spuštěním následujícího příkazu na lokálním počítači brány:
   - Linux

   ```
   sudo systemctl start faspio-gateway
   ```

5. Spusťte vzdálenou bránu spuštěním následujícího příkazu na počítači vzdálené brány:
   - Linux

   ```
   sudo systemctl start faspio-gateway
   ```

6. Restartujte kanály.

Jak pokračovat dále

Aspera gateway předává data, která přijímá, aniž by je jakýmkoli způsobem interpretoval. To znamená, že můžete nakonfigurovat TLS mezi kanály správce front, které používají produkt Aspera gateway , protože připojení brány nezná navázání komunikace TLS. To také znamená, že správci front na libovolné podporované platformě IBM MQ mohou používat produkt Aspera gateway.

Chcete-li použít správce front s více instancemi s bránou, konfigurujte definice brány pro každou instanci správce front.

Poznámka: Produkt Aspera gateway byl testován pouze s kanály správce front. Nebyl testován s kanály klienta. Důvodem je skutečnost, že předpokládané použití produktu Aspera gateway je připojení vzdálených správců front prostřednictvím pomalé sítě, zatímco klientské aplikace se obvykle připojují ke správcům front v lokálním datovém středisku prostřednictvím rychlé sítě.

Související pojmy

Orientační plán analyzátoru Aspera gateway

Související odkazy

“Jaký typ komunikace použít” na stránce 15
Různé platformy podporují různé komunikační protokoly. Vaše volba přenosového protokolu závisí na vaší kombinaci platformy IBM MQ MQI client a platformy serveru.

Dokumentace produktu IBM Aspera faspio Gateway

Multi Konfigurace produktu IBM MQ pro použití se službou měření IBM Cloud Private

Konfigurace produktu IBM MQ pro použití se službou měření IBM Cloud Private pro vytváření sestav a zobrazení informací o spuštění a použití správce front.

Než začnete

Před konfigurací správců front IBM MQ pro použití služby IBM Cloud Private musíte mít účet IBM Cloud . Chcete-li vytvořit svůj účet, prohlédněte si téma Registrace k produktu IBM Cloud.

Informace o této úloze

Pomocí IBM Cloud Private služby měřenímůžete připojit lokální produkty IBM k instanci služby v produktu IBM Cloud Private a zobrazit všechny registrované produkty ve vaší organizaci v jediném řídicím panelu.

Můžete konfigurovat a připojit správce front AIX, Linuxa Windows k instanci služby měření a zobrazit informace o jejich spuštění a použití. Avšak na jiných platformách, než jsou prostředí Linux Container, nelze data použít na podporu hodinových licencí na stanovení cen založených na kontejnerech.

Chcete-li zaznamenat data o využití pro měsíční typ licence VPC, místo výchozí metriky hodinového licencování, nastavte proměnnou prostředí `AMQ_LICENSING_METRIC=VPCMonthlyPeak`. To způsobí, že správce front odešle data související s měsíčními typy licencí VPC namísto výchozího chování odesílání dat souvisejících s hodinovými licencemi založenými na kontejnerech.

Použijte následující atributy se sekcí `ReportingService` v souboru `qm.ini` :

APIKeyFile
Umístění textového souboru s hodnotou **APIKey** instance služby měření.

CapacityReporting
Zapisuje zprávy protokolu chyb pravidelně do protokolů AMQERR v následujícím formátu:

```
4/22/2020 01:44:29 PM - Process(1274.1) User(bld-adm) Program(amqmgr0)
Host(8b3b83f2bc7d) Installation(Docker)
VRMF(9.2.0.0)
Time(2020-04-22T13:44:29.295Z)
ArithInsert1(300)
CommentInsert1(8.5)
CommentInsert2(IBM MQ Advanced)
```

Informace vytvořené atributem **CapacityReporting** jsou vloženy do zprávy AMQ5064, která vám poskytne lepší přehled o tom, kolik IBM MQ váš podnik používá:

AMQ5064
Tento správce front je spuštěn 300 sekund. Momentálně je spuštěn s jádry 8.5 . Typ licence je IBM MQ Advanced.

Závažnost
0: Informace

Vysvětlení
Toto je informační zpráva pro sledování využití.

Odezva
Není.

LicensingGroup
Účtovací skupina, do které patří správce front. To ovlivňuje způsob, jakým jsou data seskupena v sestavách generovaných službou měření.

ServiceURL
Servisní adresa IBM Cloud Private .

ServiceProxy
URL a port pro server proxy HTTP , který lze použít, pokud správci front nemají přímý přístup k síti, na které je spuštěna služba měření.

Můžete vidět hostitele, na kterých jsou vaše produkty nainstalovány, verze produktů, které používáte, a platformy, na kterých jsou spuštěny. Z vysokoúrovňových metrik využití, které jsou zobrazeny pro každý produkt, můžete mít přehled o tom, jak velké jsou pracovní zátěže. V systému IBM MQmůžete zjistit, kteří správci front jsou více používáni a kteří mají lehčí pracovní zátěž.

Je-li správce front konfigurován pro připojení k instanci služby měření, jsou do produktu IBM Cloud Privatenahlášeny následující informace:

- IBM MQ Název správce front
- Identifikátor správce front IBM MQ
- Kořenový adresář instalace IBM MQ
- IBM MQ instalované komponenty (název a verze)
- Název hostitele
- Název operačního systému hostitele
- Verze operačního systému hostitele
- Informace o využití jádra virtuálního procesoru (VPC) pro správce front IBM MQ

Metriky využití VPC správce front můžete monitorovat v řídicím panelu instance služby měření.

Procedura

- Konfigurujte správce front pro použití s instancí služby měření v systému IBM Cloud Private.
- Připojte se ke službě měření IBM Cloud Private prostřednictvím serveru proxy HTTP .
- Odstraňte problémy s připojením ke službě měření IBM Cloud Private .

Související odkazy
Metrika cen pro virtuální jádra procesoru (VPC)

Multi Konfigurace správce front pro použití s instancí služby měření v systému IBM Cloud Private

Nastavte informace o zabezpečení a registraci produktu IBM Cloud pro svého správce front a poté se připojte k instanci služby měření, kterou jste již vytvořili.

Informace o této úloze

Řídicí panel instance IBM Cloud Private služby měření zobrazuje data pouze pro správce front, kteří jsou konfigurováni tak, aby zahrnovali informace o zabezpečení a registraci produktu IBM Cloud Private .

Postup

1. Postupujte podle zdokumentovaných kroků ICP pro vytvoření ID služby na adrese: Vytvoření ID služby pomocí rozhraní IBM Cloud Private CLI.
2. Postupujte podle zdokumentovaných kroků ICP pro vytvoření klíče rozhraní API na adrese: Rozhraní API pro správu klíčů.
3. Stáhněte certifikáty TLS z klastru ICP.

Poznamenejte si umístění, kam jste stáhli certifikáty. Stažené certifikáty můžete přidat do úložiště klíčů pro svého správce front v kroku “9” na stránce 829.

4. Vytvořte textový soubor `apikeyfile.txt` a přidejte hodnotu **API key** , kterou jste zkopírovali v předchozí úloze.

   Všimněte si umístění souboru `apikeyfile.txt` , abyste k němu mohli zahrnout cestu v kroku 8. Tento soubor musí být čitelný pro uživatele správce front (*'mqm*' v systémech AIX and Linux). Soubor musí obsahovat pouze samotný soubor **API key** , nikoli informační obsah JSON, například `d9c11b45-4dda-4de4-c0b2-2e4e1004dc64`.

5. Vytvořte správce front, například *QM1*.

   Další informace naleznete v tématu Vytvoření a správa správců front na platformě Multiplatforms.

6. Spusťte správce front *QM1*.

   Další informace naleznete v tématu Spuštění správce front.

7. Před spuštěním příkazů IBM MQ nezapomeňte nastavit prostředí příkazového řádku IBM MQ .

   Spusťte příkaz **setmqenv** .

   AIX V systému AIX:

   ```
   . /usr/mqm/bin/setmqenv -s
   ```

   Linux V systému Linux:

   ```
   . /opt/mqm/bin/setmqenv -s
   ```

   Windows V systému Windows:

   ```
   "C:\Program Files\IBM\MQ\bin\setmqenv.cmd" -n installation name
   ```

8. Vytvořte úložiště údajů o důvěryhodnosti SSL pro správce front *QM1*.

   AIX Začněte vytvářet úložiště údajů o důvěryhodnosti v systému AIX:

   ```
   runmqckm -keydb -create -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
   -expire 30 -stash
   ```

   Linux V systému Linux:

   ```
   runmqckm -keydb -create -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
   -expire 30 -stash
   ```

   Windows V systému Windows:

   ```
   runmqckm -keydb -create -db "MQ data directory\qmgrs\QM1\ssl\key.kdb" -pw password -type
   cms -expire 30 -stash
   ```

9. Přidejte digitální certifikáty, které jste stáhli v kroku “3” na stránce 828, do úložiště údajů o důvěryhodnosti správce front.

   AIX V systému AIX:

   ```
   runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
   -label RootCA
   -file Download_location/RootCA.crt -format ascii -trust enable

   runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
   -label ServerCert
   -file Download_location/CERT.crt -format ascii -trust enable
   ```

Linux V systému Linux:

```
runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-label RootCA
-file Download_location/RootCA.crt -format ascii -trust enable

runmqckm -cert -add -db MQ data directory/qmgrs/QM1/ssl/key.kdb -pw password -type cms
-label ServerCert
-file Download_location/CERT.crt -format ascii -trust enable
```

Windows V systému Windows:

```
runmqckm -cert -add -db "MQ data directory\qmgrs\QM1\ssl\key.kdb" -pw password -type cms
-label RootCA
-file "Download_location\RootCA.crt" -format ascii -trust enable

runmqckm -cert -add -db "C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl\key.kdb" -pw password -type
cms -label ServerCert
-file "Download_location\CERT.crt" -format ascii -trust enable
```

10. Přidejte novou sekci `ReportingService` s cestou `apikeyfile` k souboru `qm.ini` správce front:

```
ReportingService:
   APIKeyFile=APIKey file location/apikeyfile.txt
```

11. Přidejte hodnotu **API host** do souboru `qm.ini` .

    Sekce `ReportingService` nyní obsahuje cestu k hodnotám `apikeyfile` a **API host** (**ServiceURL**):

```
ReportingService:
   APIKeyFile=APIKey file location/apikeyfile.txt
   ServiceURL=https://productinsights-api.ng.bluemix.net
```

    Uložte a ukončete soubor `qm.ini` .

12. Restartujte správce front, aby se změny projevily.

    Můžete být požádáni o udělení oprávnění procesu správce front **amqzmur0** pro přístup k síti. Přístup je nezbytný k tomu, aby správce front mohl kontaktovat službu měření.

13. Zobrazte informace o správci front *QM1* v instanci služby měření.

    Když je stav vytváření sestav aktivní, informace o spuštění a využití pro všechny integrační servery na uvedeném uzlu integrace se nahlásí službě měření. Informace o použití se aktualizují každých 15 minut.

14. Volitelné: Zastavte správce front ve vytváření sestav pro službu měření tak, že odeberete sekci `ReportingService` ze souboru `qm.ini` správce front a restartujete správce front.

15. Volitelné: Zkontrolujte diagnostické informace v souboru protokolu správce front, pokud správce front nenahlásí službě měření informace o spuštění nebo použití.

    Změnit pro AIX

    AIX V systému AIX:

```
/var/mqm/qmgrs/QM1/errors/AMQERR0*.log
```

    Linux V systému Linux:

```
/var/mqm/qmgrs/QM1/errors/AMQERR0*.log
```

    Windows V systému Windows:

```
C:\ProgramData\IBM\MQ\errors\AMQERR0*.log
```

Výsledky

Vytvořili jste instanci služby měření a nakonfigurovali jste správce front pro připojení k instanci. Informace o správci front můžete zobrazit v řídicím panelu instance služby měření.

Multi Připojení ke službě měření IBM Cloud Private prostřednictvím serveru proxy HTTP

Pokud je správce front spuštěn v systému, který nemá přímý přístup ke klastru ICP, můžete pro připojení k instanci služby měření v produktu IBM Cloud Privatepoužít server proxy HTTP , který vaše organizace poskytuje.

Než začnete

Nakonfigurovali jste zabezpečení, přidali jste adresu **API key** a adresu URL služby URL do souboru `qm.ini` pro vašeho správce front.

Informace o této úloze

Tato úloha slouží ke konfiguraci správce front pro připojení k instanci služby měření v produktu IBM Cloud Private prostřednictvím serveru proxy HTTP , který poskytuje vaše organizace.

Procedura

- Přidejte atribut serveru proxy služby do sekce registrace IBM Cloud Private vašeho souboru `qm.ini` .
  Atribut **ServiceProxy** můžete nastavit takto:
  - URL , která obsahuje předponu http:// a volitelně port. Pokud neuvedete port, použije se hodnota *1080* .

    ```
    ReportingService:
       ServiceProxy=http://myorgproxy.net:1080
    ```

  Poznámka: Parametr **ServiceProxy** musí být nastaven na platnou adresu URL http:// URL. Jiné protokoly proxy, například HTTPS a SOCKS, nejsou podporovány.
- Restartujte správce front, aby se změny projevily.

Multi Odstraňování problémů s připojením ke službě měření

Rady pro odstraňování problémů s chybami, se kterými se můžete setkat při připojování správce front k instanci služby měření.

Správce front nemůže registrovat nebo odeslat metriky využití do nakonfigurované služby měření

Zkontrolujte, zda má správce front přístup k síti. Hodnota **APIKey** v souboru s klíči rozhraní API je chybná. Ujistěte se, že je nainstalována komponenta IBM Global Security Kit (GSKit) .

Neplatná sekce `qm.ini`

Byla nalezena neplatná sekce `qm.ini` . Další informace naleznete v protokolu chyb.

Neplatný parametr serveru proxy služby HTTP

Hodnota atributu **ServiceProxy** pro sekci `ReportingService` správce front není správně nakonfigurována. Správce front se ve službě neregistrují. Parametr **ServiceProxy** musí být nastaven na platnou adresu URL http:// . Jiné protokoly proxy, například HTTPS a SOCKS, nejsou podporovány.

Deprecated Linux Konfigurace produktu IBM MQ pro použití s Salesforce tématy typu push a událostmi platformy

Tyto informace použijte k nastavení zabezpečení a připojení k produktu Salesforce a vaší síti IBM MQ pomocí konfigurace a následného spuštění serveru IBM MQ Bridge to Salesforce.

Než začnete

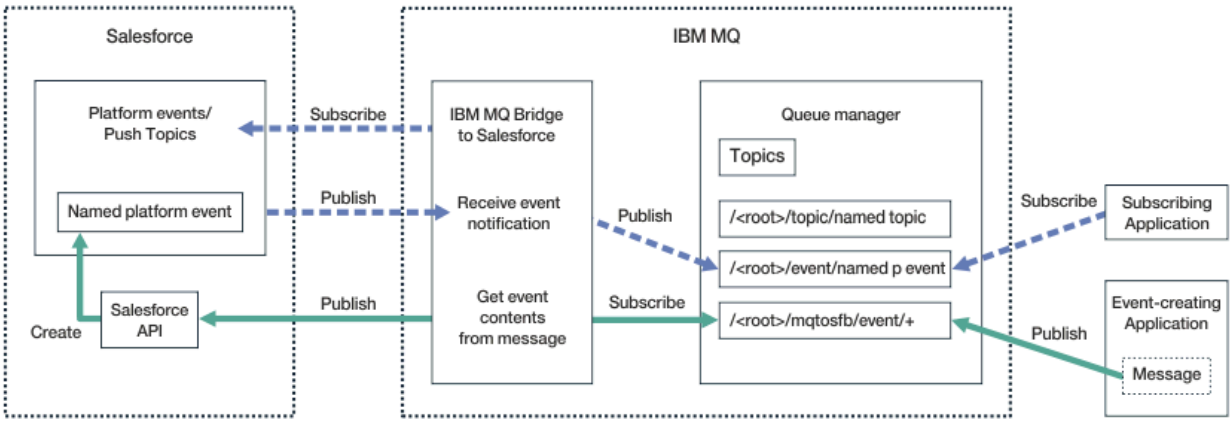
Poznámka: Deprecated Produkt IBM MQ Bridge to Salesforce je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-341). Salesforce konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo prostřednictvím App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.

- IBM MQ Bridge to Salesforce je k dispozici na systému Linux pro x86-64 (64bitový). Most není podporován pro připojení ke správcům front, kteří jsou spuštěni v systému IBM WebSphere MQ 6.0 a starším.
- V produktu IBM MQ 9.2.0 může správce front podporovat více instancí mostu, kde byly správně nakonfigurovány. Další informace viz “Další volby konfigurace pro IBM MQ Bridge to Salesforce” na stránce 838.
- Nainstalujte balík **MQSeriesSFBridge** . Další informace naleznete v tématu Instalace serveru IBM MQ na systémech Linux a IBM MQ komponenty rpm pro systémy Linux.

Informace o této úloze

Salesforce je cloudová platforma pro správu vztahů se zákazníky. Používáte-li produkt Salesforce ke správě zákaznických dat a interakcí, můžete použít IBM MQ Bridge to Salesforce k přihlášení k odběru Salesforce témat typu push a událostí platformy, které pak mohou být publikovány do vašeho správce front IBM MQ . Aplikace, které se připojují k tomuto správci front, mohou využívat data tématu odeslání typu push a události platformy užitečným způsobem. Můžete také použít most k vytvoření zpráv událostí pro události platformy v produktu Salesforce.

Přehled souboru IBM MQ Bridge to Salesforceviz diagram na Obrázku 1.



Obrázek 97. IBM MQ Bridge to Salesforce

Témata typu push jsou dotazy, které definujete pro použití rozhraní `Force.com` Streaming API pro příjem oznámení o změnách záznamů v produktu Salesforce. Další informace o konfiguraci témat typu push a o tom, jak používat rozhraní Streaming API, naleznete v tématu Představení rozhraní Streaming API a Práce s PushTopics.

Události platformy jsou přizpůsobitelné zprávy událostí, které lze definovat pro určení dat událostí, která platforma `Force.com` vytváří nebo spotřebovává. Další informace o událostech platformy a rozdílech

mezi událostmi produktu Salesforce naleznete v tématu Události platformy podnikového systému zpráv a Jaký je rozdíl mezi událostmi Salesforce.

- Chcete-li vytvořit konfiguraci pro přihlášení k odběru témat typu push a událostí platformy, prohlédněte si téma “Konfigurace agenta IBM MQ Bridge to Salesforce” na stránce 833.
- Chcete-li vytvořit konfiguraci pro vytváření zpráv událostí pro události platformy Salesforce , prohlédněte si téma “Vytvoření zpráv událostí pro události platformy Salesforce” na stránce 840.

Data z mostu můžete monitorovat dvěma způsoby, prostřednictvím konzoly IBM MQ Console a pomocí parametru **-p** s příkazem **amqsrua** . Pro celkový stav mostu je publikována jedna sada dat:

- Celkový počet zpráv tématu odeslání typu push, které jsou zpracovány v intervalu (pod stromem `STATUS/PUSHTOPIC`).
- Počet témat odeslání typu push, která jsou vidět v tomto intervalu.
- Celkový počet událostí platformy, které jsou zpracovány v intervalu (pod stromem `STATUS/PLATFORM`).
- Počet událostí platformy, které jsou vidět v tomto intervalu.
- Celkový počet událostí platformy IBM MQ vytvořených v intervalu (pod stromem `STATUS/MQPE`).
- Jedinečný počet událostí platformy vytvořených produktem IBM MQ , které se zobrazí v tomto intervalu.
- Počet publikování událostí platformy vytvořených produktem IBM MQ , která se v tomto intervalu nezdařila.

Pro každé nakonfigurované téma Salesforce se publikuje další zpráva. Téma IBM MQ používá úplný název tématu Salesforce a `/event` nebo `/topic` v názvu objektu:

- Počet zpráv zpracovaných v intervalu.

Chcete-li nakonfigurovat server IBM MQ Console tak, aby monitoroval data mostu, prohlédněte si kroky 9 a 10 v části Konfigurace serveru IBM MQ Bridge to Salesforce. Informace o použití příkazu **amqsrua** naleznete v tématu Monitorování IBM MQ Bridge to Salesforce.

Chcete-li nakonfigurovat a spustit IBM MQ Bridge to Salesforce, postupujte podle kroků v těchto úlohách:

Postup

1. Nakonfigurujte agenta IBM MQ Bridge to Salesforce.
2. Vytvořte zprávy událostí pro události platformy Salesforce .
3. Spusťte příkaz IBM MQ Bridge to Salesforce.

Související úlohy

Trasování IBM MQ Bridge to Salesforce

Související odkazy

runmqsfb (spusťte příkaz IBM MQ Bridge to Salesforce)

Deprecated Linux Konfigurace agenta IBM MQ Bridge to Salesforce

Můžete nakonfigurovat IBM MQ a zadat parametry IBM MQ Bridge to Salesforce pro vytvoření konfiguračního souboru a připojení Salesforce témat typu push a událostí platformy ke správci front IBM MQ .

Než začnete

Poznámka: Deprecated Produkt IBM MQ Bridge to Salesforce je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-431). Salesforce konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo prostřednictvím App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.

Před spuštěním této úlohy se ujistěte, že jste nainstalovali balík `MQSeriesSFBridge` do instalace produktu IBM MQ na platformě x86-64 Linux .

Další informace naleznete v tématu Instalace serveru IBM MQ na systémech Linux a IBM MQ komponenty rpm pro systémy Linux.

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným pro vytvoření konfiguračního souboru IBM MQ Bridge to Salesforce a úspěšné připojení k Salesforce a IBM MQ , abyste se mohli přihlásit k odběru Salesforce témat typu push a událostí platformy. Další informace o významu a volbách pro všechny parametry viz příkaz runmqsfb . Musíte zvážit své vlastní požadavky na zabezpečení a upravit parametry odpovídající vaší implementaci.

Chcete-li vytvořit konfiguraci pro vytváření zpráv událostí pro události platformy Salesforce , prohlédněte si téma "Vytvoření zpráv událostí pro události platformy Salesforce" na stránce 840.

Přihlášení k odběru témat Salesforce push a událostí platformy

Když produkt IBM MQ Bridge to Salesforce vytvoří připojení jak k produktu Salesforce , tak k produktu IBM MQ, vytvoří odběry pro Salesforce témata typu push a události platformy. Název tématu odeslání typu push nebo události platformy, k jejichž odběru se chce most přihlásit, musí být zahrnut v konfiguračním souboru nebo přidán do příkazového řádku před vytvořením připojení.

Jedním z atributů konfigurace je kořen stromu témat IBM MQ a události jsou publikovány pod tímto kořenem. Most přistupuje k tomuto kořenovému adresáři a přidává úplný název tématu Salesforce , například `/MQ/SF/ROOT/topic/EscalatedCases`. Téma monitorování a aplikace, které se připojují k produktu IBM MQ , mohou hledat témata typu push v části `/topic/EscalatedCases` a události platformy v části `/event/NewCustomer__e`.

Publikovaná zpráva obsahuje řídicí informace a datovou strukturu, která obsahuje požadovaná datová pole. V případě témat typu push je struktura dat **`sobject`** a v případě událostí platformy je struktura **`payload`**. Most se nemůže přihlásit k odběru tématu nebo události, pokud nejsou definovány v souboru Salesforce. Pokud most při pokusu o přihlášení k odběru tématu narazí na chybu, most se zastaví.

Objekt tématu nemusí být definován v souboru IBM MQ , ale musí existovat vhodná oprávnění na základě nejbližšího nadřízeného prvku ve stromu. Znovu publikovanou zprávu standardně obsahuje pouze relevantní datovou strukturu z původní zprávy. Řídicí informace jsou odebrány. V případě událostí platformy má publikace strukturu informačního obsahu. Volba konfigurace **`Publish control data with the payload`** v sadě konfiguračních parametrů **Chování programu mostu** umožňuje opětovné publikování celé zprávy včetně řídicích dat. Další informace viz Konfigurační parametry.

Každé téma odeslání typu push a událost platformy mají přidružené *ReplayID* při publikování z Salesforce. *ReplayID* lze použít k vyžádání počátečního bodu pro publikování, když je vytvořeno připojení k serveru. Produkt Salesforce udržuje historii po dobu až 24 hodin a umožňuje mostu nezmeškat nedávná témata odeslání typu push a události platformy, i když nebyly spuštěny v době, kdy byly generovány. Most podporuje dva režimy kvality služeb:

Nanejvýš jednou
: Most nepoužívá pro restart *ReplayId* . Po restartu mostu se zpracují pouze nově generovaná témata odeslání typu push a události platformy. Žádosti musí být připraveny na řešení chybějících publikací. *ReplayId* je stále sledován mostem a utvrzen do fronty, takže most lze restartovat s jinou kvalitou služby a znát aktuální stav.

Nejméně jednou
: *ReplayId* je sledováno mostem a utvrzeno do fronty. Při restartu mostu se trvalé *ReplayId* používá k vyžádání počátečního bodu pro publikování ze serveru. Za předpokladu, že mezera nebyla delší než 24 hodin, odesílají se starší publikace. *ReplayId* pro téma není u každé zprávy utvrzeno. Je zapsána v trvalé zprávě v pravidelných intervalech a při vypnutí mostu. Aplikace musí být připraveny k zobrazení duplicitních publikací.

ReplayId se zapíše jako zpráva do nově definované fronty. Tuto frontu **`SYSTEM.SALESFORCE.SYNCQ`**musíte definovat před spuštěním mostu. Pokud **`SYSTEM.SALESFORCE.SYNCQ`** neexistuje, most nebude pokračovat bez ohledu na režim kvality služby. Pro vytvoření fronty s příslušnými atributy je poskytnut skript MQSC. Fronta musí být konfigurována

s volbou DEFSOPT (EXCL) NOSHARE , aby bylo zajištěno, že frontu **SYSTEM.SALESFORCE.SYNCQ** může aktualizovat pouze jedna instance programu mostu.

Chcete-li vytvořit konfiguraci pro vytváření zpráv událostí pro události platformy, prohlédněte si téma "Vytvoření zpráv událostí pro události platformy Salesforce" na stránce 840.

Postup

1. Vytvořte a spusťte správce front.
   a) Vytvořte správce front, například SQM1.

   ```
   crtmqm SQM1
   ```

   b) Spusťte správce front.

   ```
   strmqm SQM1
   ```

2. **Poznámka:** Chcete-li použít existující přihlašovací pověření a pověření zabezpečení Salesforce a certifikát podepsaný svým držitelem, přejděte na krok "3" na stránce 835.

   Volitelné: Vytvořte token zabezpečení pro svůj účet Salesforce .
   a) Přihlaste se ke svému účtu Salesforce .
   b) Vytvořte nebo resetujte token zabezpečení podle kroků v nápovědě Salesforce : Resetovat token zabezpečení.
3. Vytvořte bezpečnostní certifikát podepsaný certifikační autoritou v adresáři Salesforce.
   a) Vyberte volbu **Řízení zabezpečení** v nabídce **Spravovat** na stránce **Force.com Domovská stránka** a poté volbu **Správa certifikátů a klíčů**.

   Otevře se stránka **Správa certifikátů a klíčů** .
   b) Klepněte na volbu **Vytvořit certifikát podepsaný certifikační autoritou**.

   Otevře se stránka **Certifikáty** .
   c) Do pole **Popisek** zadejte název certifikátu, stiskněte klávesu Taba klepněte na tlačítko **Uložit**.

   Zobrazí se informace o podrobnostech certifikátu a klíče.
   d) Klepněte na tlačítko **Zpět na seznam: Certifikáty a klíče**.
   e) Klepněte na volbu **Exportovat do úložiště klíčů**.
   f) Zadejte heslo úložiště klíčů a poté klepněte na volbu **Exportovat**.
   g) Uložte exportované úložiště klíčů do lokálního systému souborů.
4. Pomocí grafického rozhraní správy klíčů IBM otevřete úložiště klíčů, které jste exportovali z produktu Salesforce , a naplňte certifikáty podepsaného.
   a) Spusťte příkaz **strmqikm** a otevřete grafické rozhraní produktu IBM Key Management.

   Další informace naleznete v tématu Použití příkazu runmqckm, runmqakm a strmqikm ke správě digitálních certifikátů.
   b) Klepněte na volbu **Otevřít soubor databáze klíčů** a vyhledejte umístění úložiště klíčů Salesforce .
   c) Klepněte na tlačítko **Otevřít**, ujistěte se, že jste vybrali volbu **JKS** z voleb **Typ databáze klíčů** , pak klepněte na tlačítko **OK**.
   d) Zadejte heslo, které jste vytvořili pro úložiště klíčů v kroku 3f, a poté klepněte na tlačítko **OK**.
   e) Ve volbách **Obsah databáze klíčů** vyberte volbu **Certifikáty podepsaného** .
   f) Klepněte na volbu **Naplnit**.
   g) V seznamu **Přidat certifikáty CA** zaškrtněte políčko **Verisign Inc.** a klepněte na tlačítko **OK**.
5. Volitelné: Vygenerujte klíč a tajný údaj spotřebitele OAuth vytvořením připojení aplikace pro IBM MQ Bridge to Salesforce ve vašem účtu Salesforce .

   Při používání produktu IBM MQ Bridge to Salesforce v produkčních prostředích potřebujete kódy **Klíč spotřebitele** a **Utajený údaj spotřebitele** .

a) Vyberte volbu **Vytvořit**a poté **Aplikace** z nabídky **Sestavit** na vaší stránce **Force.com Domů** .

Otevře se stránka Aplikace.

b) V sekci **Připojené aplikace** klepněte na volbu **Nový** .

Otevře se stránka **Nová připojená aplikace** .

c) Do pole **Název připojené aplikace**zadejte název IBM MQ Bridge to Salesforce , například **MQBridgeToSalesforce**.

d) Zadejte **Název rozhraní API**.

Pokud přejdete na další pole, **Název připojené aplikace** se zkopíruje do pole názvu **Název rozhraní API** .

e) Zadejte svůj **Kontaktní e-mail**.

f) Vyberte volbu **Povolit nastavení OAuth** v sekci **API (Povolit nastavení OAuth)** .

Další možnosti v této sekci jsou pak prezentovány.

g) Přidejte adresu URL **Callback URL**, například `https://www.ibm.com`.

h) Vyberte volbu **Úplný přístup (plný)** ze seznamu **Dostupné rozsahy OAuth** v podsekci **Vybrané rozsahy OAuth** a poté klepněte na tlačítko **Přidat**, abyste přidali úplný přístup do seznamu **Vybrané rozsahy OAuth** .

i) Klepněte na tlačítko **Uložit**.

j) Klepněte na tlačítko **Pokračovat**.

k) Poznamenejte si kódy **Klíč spotřebitele** a **Utajený údaj spotřebitele** .

6. Vytvořte požadovanou frontu synchronizace ve správci front.

```
cat /opt/mqm/mqsf/samp/mqsfbSyncQ.mqsc | runmqsc SQM1
```

Fronta synchronizace udržuje stav událostí v rámci restartů aplikace nebo správce front. Hloubka fronty může být malá, protože ve frontě se očekává pouze jedna zpráva. Pro tuto frontu může být v daném okamžiku spuštěna pouze jedna instance mostu, takže výchozí volby jsou nastaveny pro výlučný přístup.

7. Vytvořte konfigurační soubor s parametry připojení a zabezpečení pro chování IBM MQ, Salesforcea IBM MQ Bridge to Salesforce .

```
runmqsfb -o new_config.cfg
```

Existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte klávesu `Enter` , abyste přijali existující hodnoty, stiskněte klávesu `Space` a poté `Enter` , abyste vymazali hodnoty, a zadejte `Enter` , abyste přidali nové hodnoty.

a) Zadejte hodnoty pro připojení ke správci front SQM1:

Minimální hodnoty potřebné pro připojení jsou název správce front, kořenový adresář základního tématu IBM MQ a název kanálu.

```
Connection to Queue Manager
---------------------------
Queue Manager or JNDI CF   : []SQM1
MQ Base Topic              : []/sf
MQ Channel                 : []A channel you have defined or for example
SYSTEM.DEF.SVRCONN
MQ Conname                 : []
MQ Publication Error Queue : [SYSTEM.SALESFORCE.ERRORQ]
MQ CCDT URL                : []
JNDI implementation class  : [com.sun.jndi.fscontext.RefFSContextFactory]
JNDI provider URL          : []
MQ Userid                  : []
MQ Password                : []
```

Poznámka: Název kanálu není vyžadován, pokud se připojujete lokálně. Nemusíte zadat název správce front a základní téma v konfiguračním souboru, protože je lze později při spuštění mostu zahrnout do příkazového řádku.

b) Zadejte hodnoty pro připojení k Salesforce:

Minimální hodnoty potřebné pro připojení jsou Salesforce ID uživatele, heslo, token zabezpečení a koncový bod přihlášení. V produkčních prostředích můžete přidat klíč spotřebitele a tajný údaj pro zabezpečení OAuth.

```
Connection to Salesforce
------------------------
Salesforce Userid (reqd)   : []salesforce_login_email
Salesforce Password (reqd) : []salesforce_login_password
Security Token (reqd)      : []Security_Token
Login Endpoint             : [https://login.salesforce.com]
Consumer ID                : []
Consumer Secret Key        : []
```

c) Zadejte hodnoty pro úložiště certifikátů pro připojení TLS:

Minimální hodnoty potřebné pro připojení TLS jsou cesta k úložišti klíčů pro certifikáty TLS a heslo úložiště klíčů. Není-li zadána žádná cesta k důvěryhodnému úložišti ani heslo, budou pro důvěryhodné úložiště a heslo použity parametry úložiště klíčů a hesla. Pokud používáte TLS pro připojení správce front IBM MQ , můžete použít stejné úložiště klíčů.

```
Certificate stores for TLS connections
--------------------------------------
Personal keystore for TLS certificates : []path_to_keystore, for example: /var/mqm/qmgrs/
SQM1/ssl/key.jks
Keystore password          : []keystore_password
Trusted store for signer certificates : []
Trusted store password     : []
Use TLS for MQ connection  : [N]
```

d) Zadejte hodnoty pro konfiguraci chování konzoly IBM MQ Bridge to Salesforce:

Nemusíte měnit ani poskytovat žádnou z těchto hodnot, ale pokud znáte názvy témat odeslání typu push nebo událostí platformy, přidejte je sem. Mohou být také přidány později, v příkazovém řádku, když jste připraveni spustit most. Musíte uvést soubor protokolu, v konfiguračním souboru nebo na příkazovém řádku.

```
Behaviour of bridge program
---------------------------
PushTopic Names          : []
Platform Event Names     : []
MQ Monitoring Frequency  : [30]
At-least-once delivery? (Y/N) : [Y]
Subscribe to MQ publications for platform events? (Y/N) : [N]
Publish control data with the payload? (Y/N) : [N]
Delay before starting to process events : [0]
Runtime logfile for copy of stdout/stderr : []
```

8. Volitelné: Vytvořte službu IBM MQ pro řízení provádění programu. Upravte ukázkový soubor `mqsfbService.mqsc` tak, aby ukazoval na nově vytvořený konfigurační soubor, a proveďte další změny parametrů příkazu.

```
cat modified mqsfbService.mqsc | runmqsc SQM1
```

9. Volitelné: Při nastavování konzoly IBM MQ Consolepostupujte podle pokynů v části Začínáme s konzolou IBM MQ .

10. Volitelné: Nakonfigurujte IBM MQ Bridge to Salesforce tak, aby se spouštěli jako uživatel bez kořene.

Aby bylo možné spustit IBM MQ Bridge to Salesforce jako *uživatel bez kořene*, například v *kontejneru bez kořene*, musí být správně nastaveny adresáře Java `userRoot` a `systemRoot` , aby byl zajištěn přístup pro čtení/zápis pro uživatele, který spouští proces mostu. Chcete-li to provést, nastavte následující vlastnosti prostředí JVM:

```
export MQSFB_EXTRA_JAVA_OPTIONS="-
Djava.util.prefs.userRoot=directory_with_read_write_access"
```

```
export MQSFB_EXTRA_JAVA_OPTIONS="-
Djava.util.prefs.systemRoot=directory_with_read_write_access"
```

Výsledky

Vytvořili jste konfigurační soubor, který produkt IBM MQ Bridge to Salesforce používá k odběru témat typu push a událostí platformy Salesforce , a publikovali jste je ve své síti IBM MQ .

Jak pokračovat dále

Projděte kroky pro “Spuštění prostředí IBM MQ Bridge to Salesforce” na stránce 846.

Související úlohy

Trasování IBM MQ Bridge to Salesforce

Monitorování produktu IBM MQ Bridge to Salesforce

Související odkazy

runmqsfb (spusťte příkaz IBM MQ Bridge to Salesforce)

Deprecated Linux Další volby konfigurace pro IBM MQ Bridge to Salesforce

V produktu IBM MQ 9.2.0jsou k dispozici další volby konfigurace, které povolují dvě hlavní třídy další topologie, které se zabývají "příchozími" (události generované z produktu Salesforce, publikované do aplikací IBM MQ) a "odchozími" (aplikaceIBM MQ publikující události odeslané do produktu Salesforce). Kromě toho dochází ke změně způsobu, jakým trasování a protokolování funguje.

Změny z konzoly IBM MQ 9.1.0 IBM MQ Bridge to Salesforce

V produktu IBM MQ 9.2.0se standardně neprovádí žádné změny chování z mostu IBM MQ 9.1.0 , kromě souboru protokolu, který začíná rotovat. Další informace viz “Výměnné protokoly” na stránce 839.

Hlavní změnou je, že správce front podporuje více instancí mostu. Chcete-li povolit tuto funkci a zbytek dalších topologií, musíte provést některé ruční změny konfigurace.

Další informace o dalších volbách konfigurace viz runmqfsb a příklad revidovaných informací o konfiguraci “Příklad výstupu konfigurace pro IBM MQ Bridge to Salesforce” na stránce 840 .

Oddělená příchozí práce

Více instancí mostu může zpracovat příchozí práci z Salesforce do IBM MQ, ale musí pracovat na nezávislých sadách témat a událostí typu push Salesforce . Jinak by existovala možnost, že by aplikace IBM MQ viděly opakované události, protože neexistuje žádný protokol křížového mostu, který by zastavil duplikaci událostí. Každá instance používá vlastní konfigurovatelnou frontu synchronizace k zadržení **ReplayId**.

To je pravděpodobně užitečné, když:

- Různá témata produktu Salesforce mají různá bezpečnostní oprávnění. Každá instance mostu má jinou sadu pověření pro přístup k produktu Salesforce.
- Máte obavy z toho, že pracovní zátěž pochází z toho, že produkt Salesforce je příliš velký na to, aby zvládl jeden most. Proto můžete uspořádat témata, která mají být rozdělena s "A-M" procházející jedním mostem a "N-Z" přes jiný.

Sdílená odchozí práce

Most podporuje více instancí pro podporu odchozí práce odesílané z IBM MQ do Salesforce. Dojde-li k selhání jedné instance mostu, mohou ostatní instance přihlášené k odběru stejných témat ve stejném správci front pokračovat ve zpracování publikování.

Poznámka: Pro tento účel nejsou potřeba žádné změny konfigurace tématu IBM MQ .

Tyto spolupracující instance musí být nastaveny tak, aby maximálně jedna z instancí zpracovala příchozí práci z produktu Salesforce, protože tato instance musí mít výlučný přístup k frontě synchronizace.

To je pravděpodobné, že bude užitečné, pokud máte obavy o:

- Pracovní zátěž pochází z IBM MQ. Vzhledem k tomu, že požadavky na Salesforce jsou synchronní, most nemůže zpracovat novou práci, zatímco stále zpracovává jednu zprávu. Mít více spotřebitelů tuto situaci zmírňuje.
- Architektura dostupnosti. Nyní je například možné spustit více instancí v samostatných datových střediscích s lepšími možnostmi překonání selhání a zotavení z havárie. Spuštění jako klient IBM MQ také odděluje most od umístění správce front.

Interakce trasování a ladění

V produktu IBM MQ 9.2.0se příznak ladění i nadále bude chovat jako v případě IBM MQ 9.1.0. To znamená, že *-d1* poskytuje informace o ladění mostu a *-d2* zapíná protokolování ladění pro nezbytné komponenty. Pokud jste však při spuštění mostu povolili trasování systému IBM MQ , bude vytváření sestav na úrovni *-d2* automaticky zapnuto.

Výměnné protokoly

V systému IBM MQ 9.2.0je výchozím chováním souboru protokolu tři soubory protokolu, každý o velikosti 2 MB. Tyto hodnoty můžete přepsat pomocí dalších vlastností konfigurace. Existující atribut konfigurace nebo parametr příkazového řádku pro soubor protokolu je považován za základní název protokolů s přidaným indexem.

Pokud má nakonfigurovaný soubor protokolu:

- Žádný typ souboru, index se přidá na konec názvu souboru.

  Nastavení souboru protokolu na hodnotu `abc`vede k protokolům s názvem `abc.0`, `abc.1`atd.
- Typ souboru, index je vložen před typ souboru.

  Nastavení souboru protokolu na hodnotu `abc.log`vede k protokolům s názvem `abc.0.log`, `abc.1.log`atd.

Notes:

1. Vzhledem k tomu, že mosty mohou být spuštěny s libovolným oprávněním uživatele, není možné vynutit určitý adresář, například `/var/mqm/qmgrs/<qm>/errors`, pro protokoly.
2. Stejné informace se i nadále zapisují do proudů *stdout* a *stderr* .
3. Při každém opětovném otevření jednotlivého souboru protokolu se znovu vytisknou základní informace o konfiguraci. Informace budou vždy k dispozici, místo aby byly vytištěny pouze jednou na začátku programu.

Zachování protokolů

Vzhledem k topologiím systému IBM MQ 9.2.0 je pravděpodobnější, že pro konkrétního správce front bude spuštěno více instancí mostu.

Aby se zabránilo vzájemnému rušení instancí a aby se zabránilo přepsání předchozích spuštění mostu, most se nespustí, pokud již existuje protokol `.0` .

Před spuštěním mostu potřebujete spouštěcí proceduru, která odstraní předchozí kopie protokolu, nebo přidá k názvu něco jako časové razítko.

Související úlohy

“Konfigurace produktu IBM MQ pro použití s Salesforce tématy typu push a událostmi platformy” na stránce 832
Tyto informace použijte k nastavení zabezpečení a připojení k produktu Salesforce a vaší síti IBM MQ pomocí konfigurace a následného spuštění serveru IBM MQ Bridge to Salesforce.

Trasování produktu IBM MQ Bridge to Salesforce

Související odkazy

runmqfsb

Deprecated Linux Příklad výstupu konfigurace pro IBM MQ Bridge to Salesforce

Příklad výstupu konfigurace zobrazující změny z IBM MQ 9.1.0 IBM MQ Bridge to Salesforce.

```
IBM MQ Bridge to Salesforce
5724-H72 (C) Copyright IBM Corp. 2017, 2024.
Level : <<unknown>>

Enter new values for the configuration attributes. The
current settings are shown.
Press ENTER to accept current values; use SPACE+ENTER
to clear values.

Connection to Queue Manager
---------------------------
Queue Manager or JNDI CF   : [V9000_A]
MQ Base Topic              : [/sf]
MQ Channel                 : []
MQ Conname                 : []
MQ Publication Error Queue : [SYSTEM.SALESFORCE.DEADQ]
MQ Replay Status Queue     : [SYSTEM.SALESFORCE.SYNCQ]
MQ CCDT URL                : []
JNDI implementation class  : [com.sun.jndi.fscontext.RefFSContextFactory]
JNDI provider URL          : []
MQ Userid                  : []
MQ Password                : []

Connection to Salesforce
------------------------
Salesforce Userid (reqd)   : [johndoe@<yourenterprise>.com]
Salesforce Password (reqd) : [********]
Security Token             : [********]
Login Endpoint             : [https://login.salesforce.com]
Consumer Key               : [3MVG9HxRZv05HarQhSy89qSKYNr1gDcv1wE3zN5kyFAa4Wxt]
Consumer Secret            : [********]

Certificate stores for TLS connections
--------------------------------------
Personal keystore for TLS certificates : [/var/mqm/ssl/key.jks]
Keystore password          : [********]
Trusted store for signer certificates : []
Trusted store password     : []
Use TLS for MQ connection  : [N]

Event processing
----------------
PushTopic Names            : []
Platform Event Names       : []
At-least-once delivery for Salesforce events? (Y/N) : [N]
At-least-once delivery for MQ publications? (Y/N) : [N]
Subscribe to MQ publications for platform events? (Y/N) : [Y]
Publish control data with the payload? (Y/N) : [Y]
Treat unknown Salesforce topic as warning (Y/N) : [N]

Behaviour of bridge program
---------------------------
Bridge unique identifier   : []
MQ Monitoring Frequency    : [30]
Delay before starting to process events : [0]
Continue to retry after maximum reconnection attempts (Y/N) : [N]
Runtime logfile for copy of stdout/stderr : [/tmp/runmqsfb.log]
Number of logfiles         : [3]
Maximum size of each logfile : [2097152]
Done.
```

Související odkazy

runmqfsb

Deprecated Linux Vytvoření zpráv událostí pro události platformy Salesforce

Můžete nakonfigurovat IBM MQ a zadat `IBM MQ Bridge to Salesforce parameters`, chcete-li vytvořit konfigurační soubor a použít most k vytvoření zpráv událostí pro události platformy Salesforce .

Než začnete

- Nainstalovali jste balík **MQSeriesSFBridge** do instalace produktu IBM MQ na platformě x86-64 Linux .

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným pro vytvoření konfiguračního souboru IBM MQ Bridge to Salesforce a úspěšné připojení k Salesforce a IBM MQ , abyste mohli vytvářet zprávy událostí pro události platformy Salesforce . Další informace o významu a volbách pro všechny parametry viz příkaz runmqsfb . Musíte zvážit své vlastní požadavky na zabezpečení a upravit parametry odpovídající vaší implementaci.

Chcete-li vytvořit konfiguraci pro přihlášení k odběru témat typu push a událostí platformy, prohlédněte si téma “Konfigurace agenta IBM MQ Bridge to Salesforce” na stránce 833.

Vytvoření zpráv událostí pro události platformy Salesforce

Pomocí aplikace IBM MQ můžete vytvářet zprávy, které jsou vloženy do tématu správce front `/root/mqtosfb/event/+`. Most odebírá téma, získává obsah ze zpráv a používá jej k publikování zpráv událostí pro událost platformy Salesforce . Další informace o událostech platformy naleznete v tématu Doručení vlastních oznámení s událostmi platformy v dokumentaci vývojáře Salesforce .

Chcete-li mostu povolit vytváření zpráv událostí, musíte poskytnout dva atributy, které jsou dodatečné k atributům používaným pro přihlášení k odběru témat typu push a událostí platformy:

- Vytvořte a přidejte název položky **MQ Publication Error Queue** v atributech konfigurace mostu pro volbu **Připojení ke správci front**.
- Nastavte volbu **Subscribe to MQ publications for platform events** na hodnotu *Y*v atributech konfigurace mostu pro definování **Chování programu mostu**.

Musíte vytvořit událost platformy v produktu Salesforce a definovat pole obsahu, než budete moci použít most k vytvoření zpráv události pro tuto událost platformy. Název události platformy a její obsah určují, jak je třeba formátovat zprávu IBM MQ zpracovanou mostem. Pokud je například vaše Salesforce událost platformy **Object name** *MQPlatformEvent1* a vaše dvě vlastní definovaná pole jsou textová pole s **API name** *MyText__c* a *Name__c*, pak vaše zpráva IBM MQ , která je publikována v tématu `/root/mqtosfb/event/MQPlatformEvent1__e` , musí být ve správném formátu JSON:

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

Zpráva musí být formátována tak, aby ji produkt IBM MQ Bridge to Salesforce mohl rozpoznat jako tělo zprávy formátované pomocí MQFMT_STRING.

Viz krok “7” na stránce 843 , chcete-li vytvořit událost platformy v produktu Salesforce , nebo tento krok přeskočte, pokud již máte událost platformy, pro kterou chcete vytvořit zprávy události. Zprávu IBM MQ musíte formátovat tak, aby odpovídala polím nastaveným v události platformy Salesforce . Pole v rámci události platformy Salesforce mohou být označena jako volitelná nebo povinná. Další informace viz Pole událostí platformy v dokumentaci vývojáře Salesforce .

Když je most spuštěn, přihlásí se k odběru určeného tématu IBM MQ .

- Pokud v konfiguraci mostu určíte kvalitu služby **At-most-once** , bude odběr, který most vytváří, netrvalý. Publikování, která jsou vytvořena aplikacemi IBM MQ v době, kdy není most spuštěn, nejsou zpracována.
- Určíte-li kvalitu služby **At-least-once** v konfiguraci mostu, odběr, který most vytváří, je trvalý. To znamená, že most může zpracovávat publikování, která jsou vytvořena aplikacemi IBM MQ , zatímco most není spuštěn. Trvalé odběry vyžadují známý odběr a ID klienta. Most používá *D_SUB_RUNMQSFB* jako název odběru a *runmqsfb_1* jako ID klienta.

Pokud se most používá k přihlášení k odběru témat Salesforce typu push a událostí platformy, a nikoli k vytváření zpráv událostí, pokusí se odstranit trvalý odběr v případě změny konfigurace a odběr je nyní osiřelý.

Trvalé odběry, které most vytvoří, můžete odebrat následujícím způsobem:

Použijte IBM MQ Explorer.
Otevřete **složku odběrů** pro správce front, kterého most používá, a vyhledejte název odběru, který končí na *:D_SUB_RUNMQSFB* , kde je řetězec tématu `/sf/mqtosfb/event+`. Klepněte pravým tlačítkem myši na název odběru a klepněte na tlačítko Odstranit. Pokud se zobrazí chyba, která označuje, že je odběr používán, je možné, že most stále běží. Zastavte most a zkuste odběr odstranit znovu.

Pomocí volby `runmqsc` vyhledejte a odstraňte odběr.
Spusťte rozhraní **`runmqsc`** a spusťte příkaz `DISPLAY SUB (*)`. Vyhledejte název odběru **SUB** končící na *:D_SUB_RUNMQSFB*. Zadejte příkaz delete sub a uveďte **SUBID** odběru, který chcete odstranit. Například `DELETE SUB SUBID(414D5120514D312020202020202020205C589459987E8620)`

Zastavte a poté spusťte most s kvalitou služeb `At-most-once` .
Pokud jste spustili most s **`At-least-once`** kvalitou služby `At-least-once delivery? (Y/N) : [Y]`, vytvořený odběr je trvalý. Chcete-li odstranit odběr, změňte kvalitu služby v konfiguračním souboru na `At-least-once delivery? (Y/N) :[N]` a restartujte most. Trvalý odběr je odstraněn a je vytvořen trvalý odběr.

Postup

1. Vytvořte a spusťte správce front.
   a) Vytvořte správce front, například PEQM1.
   ```
   crtmqm PEQM1
   ```
   b) Spusťte správce front.
   ```
   strmqm PEQM1
   ```
2. **Poznámka:** Chcete-li použít existující přihlašovací pověření a pověření zabezpečení Salesforce a certifikát podepsaný svým držitelem, přejděte na krok 4.

   Volitelné: Vytvořte token zabezpečení pro svůj účet Salesforce .
   a) Přihlaste se ke svému účtu Salesforce .
   b) Vytvořte nebo resetujte token zabezpečení podle kroků v nápovědě Salesforce : Resetovat token zabezpečení.
3. Vytvořte certifikát zabezpečení podepsaný svým držitelem v adresáři Salesforce.
   a) Vyberte volbu **Řízení zabezpečení** v nabídce **Spravovat** na stránce **Force.com Domovská stránka** a poté volbu **Správa certifikátů a klíčů**.

      Otevře se stránka **Správa certifikátů a klíčů** .
   b) Klepněte na volbu **Vytvořit certifikát podepsaný držitelem**.

      Otevře se stránka **Certifikáty** .
   c) Do pole **Popisek** zadejte název certifikátu, stiskněte klávesu Taba klepněte na tlačítko **Uložit**.

      Zobrazí se informace o podrobnostech certifikátu a klíče.
   d) Klepněte na tlačítko **Zpět na seznam: Certifikáty a klíče**.
   e) Klepněte na volbu **Exportovat do úložiště klíčů**.
   f) Zadejte heslo úložiště klíčů a poté klepněte na volbu **Exportovat**.
   g) Uložte exportované úložiště klíčů do lokálního systému souborů.
4. Pomocí grafického rozhraní správy klíčů IBM otevřete úložiště klíčů, které jste exportovali z produktu Salesforce , a naplňte certifikáty podepsaného.
   a) Spusťte příkaz **`strmqikm`** a otevřete grafické rozhraní produktu IBM Key Management. Další informace naleznete v tématu Použití příkazu runmqckm, runmqakm a strmqikm ke správě digitálních certifikátů.
   b) Klepněte na volbu **Otevřít soubor databáze klíčů** a vyhledejte umístění úložiště klíčů Salesforce .

c) Klepněte na tlačítko **Otevřít**, ujistěte se, že jste vybrali volbu **JKS** z voleb **Typ databáze klíčů** , pak klepněte na tlačítko **OK**.

d) Zadejte heslo, které jste vytvořili pro úložiště klíčů v kroku 3f, a poté klepněte na tlačítko **OK**.

e) Ve volbách **Obsah databáze klíčů** vyberte volbu **Certifikáty podepsaného** .

f) Klepněte na volbu **Naplnit**.

g) V seznamu **Přidat certifikáty CA** zaškrtněte políčko **Verisign Inc.** a klepněte na tlačítko **OK**.

5. Volitelné: Vygenerujte klíč a tajný údaj spotřebitele OAuth vytvořením připojení aplikace pro IBM MQ Bridge to Salesforce ve vašem účtu Salesforce .

   Při používání produktu IBM MQ Bridge to Salesforce v produkčních prostředích potřebujete kódy **Klíč spotřebitele** a **Utajený údaj spotřebitele** .

   a) Vyberte volbu **Vytvořit**a poté **Aplikace** z nabídky **Sestavit** na vaší stránce **Force.com Domů** .

      Otevře se stránka **Aplikace** .

   b) V sekci **Připojené aplikace** klepněte na volbu **Nový** .

      Otevře se stránka **Nová připojená aplikace** .

   c) Do pole **Název připojené aplikace**zadejte název IBM MQ Bridge to Salesforce , například **MQBridgeToSalesforce**.

   d) Zadejte **Název rozhraní API**.

      Pokud přejdete na další pole, **Název připojené aplikace** se zkopíruje do pole názvu **Název rozhraní API** .

   e) Zadejte svůj **Kontaktní e-mail**.

   f) Vyberte volbu **Povolit nastavení OAuth** v sekci **API (Povolit nastavení OAuth)** .

      Další možnosti v této sekci jsou pak prezentovány.

   g) Přidejte adresu URL **Callback URL**, například `https://www.ibm.com`.

   h) Vyberte volbu **Úplný přístup (plný)** ze seznamu **Dostupné rozsahy OAuth** v podsekci **Vybrané rozsahy OAuth** a poté klepněte na tlačítko **Přidat**, abyste přidali úplný přístup do seznamu **Vybrané rozsahy OAuth** .

   i) Klepněte na tlačítko **Uložit**.

   j) Klepněte na tlačítko **Pokračovat**.

   k) Poznamenejte si kódy **Klíč spotřebitele** a **Utajený údaj spotřebitele** .

6. Vytvořte požadované fronty synchronizace a chyb ve správci front.

```
cat /opt/mqm/mqsf/samp/mqsfbSyncQ.mqsc | runmqsc PEQM1
```

   Fronta synchronizace udržuje stav událostí v rámci restartů aplikace nebo správce front. Hloubka fronty může být malá, protože ve frontě se očekává pouze jedna zpráva. Pro tuto frontu může být v daném okamžiku spuštěna pouze jedna instance mostu, takže výchozí volby jsou nastaveny pro výlučný přístup. Před použitím mostu k vytvoření zpráv událostí pro události platformy musí být vytvořena fronta chyb. Fronta chyb se používá pro zprávy, které nelze úspěšně zpracovat produktem Salesforce. Musíte přidat název fronty chyb do sekce konfiguračního parametru mostu **`Connection to Queue Manager`** , jak ukazuje krok “8.a” na stránce 844.

7. Volitelné: Vytvořte objekt události platformy ve svém účtu Salesforce .

   a) Vyberte volbu **Události platformy** v nabídce **Vývoj** na stránce **Force.com Domů** a poté klepněte na volbu **Nová událost platformy**.

      Otevře se stránka **Nová událost platformy** .

   b) Vyplňte pole **Popisek** a **Plurální popisek** .

   c) Klepněte na tlačítko **Uložit**.

      Otevře se stránka **Podrobnosti definice události platformy** .

   d) Definujte **Vlastní pole a vztahy**.

Můžete například přidat dvě textová pole s popisky *MyText* a *Název* a nastavit délku pole **Datový typ** na *Text (64)* a hodnotu *Text (32)* .

Vytvořili jste událost platformy a definovali jste pro ni **Custom Fields and Relationships** . Použijte událost platformy *Název objektu platformy* nebo *Název rozhraní API* jako téma IBM MQ , do kterého můžete vložit zprávy, které má most zpracovat. Například můžete použít ukázku **AMQSPUBA** k přidání následující zprávy ve formátu JSON do tématu `/sf/mqtosfb/event/`*`Salesforce Platform Object Name/API name`* :

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

Po spuštění mostu můžete spustit ukázku **AMQSPUBA** a vytvořit zprávy. V adresáři *`MQ installation location`*`/samp/bin` zadejte následující příkaz:

```
./amqspub /sf/mqtosfb/event/Salesforce Platform Object Name/API name PEQM1
```

Na výzvu zadejte zprávu ve formátu JSON.

8. Vytvořte konfigurační soubor s parametry připojení a zabezpečení pro chování IBM MQ, Salesforcea IBM MQ Bridge to Salesforce .

```
runmqsfb -o new_config.cfg
```

Existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte klávesu `Enter` , abyste přijali existující hodnoty, stiskněte klávesu `Space` a poté `Enter` , abyste vymazali hodnoty, a zadejte `Enter` , abyste přidali nové hodnoty.

a) Zadejte hodnoty pro připojení ke správci front PEQM1:

Minimální hodnoty potřebné pro připojení jsou název správce front, kořen základního tématu IBM MQ , název fronty chyb a název kanálu.

```
Connection to Queue Manager
---------------------------
Queue Manager or JNDI CF   : []PEQM1
MQ Base Topic              : []/sf
MQ Channel                 : []A channel you have defined or for example
SYSTEM.DEF.SVRCONN
MQ Conname                 : []
MQ Publication Error Queue : [SYSTEM.SALESFORCE.ERRORQ]
MQ CCDT URL                : []
JNDI implementation class  : [com.sun.jndi.fscontext.RefFSContextFactory]
JNDI provider URL          : []
MQ Userid                  : []
MQ Password                : []
```

Poznámka: Pokud se připojujete lokálně, název kanálu není povinný. Nemusíte zadat název správce front a základní téma v konfiguračním souboru, protože je lze později při spuštění mostu zahrnout do příkazového řádku.

b) Zadejte hodnoty pro připojení k Salesforce:

Minimální hodnoty potřebné pro připojení jsou Salesforce ID uživatele, heslo, token zabezpečení a koncový bod přihlášení. V produkčních prostředích můžete přidat klíč spotřebitele a tajný údaj pro zabezpečení OAuth.

```
Connection to Salesforce
------------------------
Salesforce Userid (reqd)   : []salesforce_login_email
Salesforce Password (reqd) : []salesforce_login_password
Security Token (reqd)      : []Security_Token
Login Endpoint             : [https://login.salesforce.com]
Consumer ID                : []
Consumer Secret Key        : []
```

c) Zadejte hodnoty pro úložiště certifikátů pro připojení TLS:

Minimální hodnoty potřebné pro připojení TLS jsou cesta k úložišti klíčů pro certifikáty TLS a heslo úložiště klíčů. Není-li zadána žádná cesta k důvěryhodnému úložišti ani heslo, budou

pro důvěryhodné úložiště a heslo použity parametry úložiště klíčů a hesla. Pokud používáte TLS pro připojení správce front IBM MQ , můžete použít stejné úložiště klíčů.

```
Certificate stores for TLS connections
--------------------------------------
Personal keystore for TLS certificates : []path_to_keystore, for example: /var/mqm/qmgrs/
PEQM1/ssl/key.jks
Keystore password          : []keystore_password
Trusted store for signer certificates : []
Trusted store password     : []
Use TLS for MQ connection  : [N]
```

d) Zadejte hodnoty pro konfiguraci chování konzoly IBM MQ Bridge to Salesforce:

Chcete-li použít most k vytváření zpráv událostí, musíte změnit volbu **Subscribe to MQ publications for platform events** z výchozího *N*na *Y* . Musíte také uvést soubor protokolu, v konfiguračním souboru nebo na příkazovém řádku.

```
Behaviour of bridge program
---------------------------
PushTopic Names             : []
Platform Event Names        : []
MQ Monitoring Frequency     : [30]
At-least-once delivery? (Y/N) : [Y]
Subscribe to MQ publications for platform events? (Y/N) : [Y]
Publish control data with the payload? (Y/N) : [N]
Delay before starting to process events : [0]
Runtime logfile for copy of stdout/stderr : []
```

9. Volitelné: Vytvořte službu IBM MQ pro řízení provádění programu. Upravte ukázkový soubor `mqsfbService.mqsc` tak, aby ukazoval na nově vytvořený konfigurační soubor, a proveďte další změny parametrů příkazu.

```
cat modified mqsfbService.mqsc | runmqsc PEQM1
```

10. Volitelné: Při nastavování konzoly IBM MQ Consolepostupujte podle pokynů v části Začínáme s konzolou IBM MQ .
11. Volitelné: Přidejte a nakonfigurujte moduly widget ve své instanci IBM MQ Console pro zobrazení dat Salesforce .
    a) Klepněte na volbu **Přidat modul widget**.

    Otevře se nový modul widget.

    b) Vyberte volbu **Grafy** .

    c) Klepněte na ikonu **Konfigurovat modul widget** v pruhu titulku nového modulu widget.

    d) Volitelné: Zadejte **Název modulu widget**.

    e) Z rozevírací nabídky **Prostředek k monitorování**, **Zdroj** vyberte volbu **Salesforce Salesforce** .

    f) V rozevírací nabídce **Třída prostředků**vyberte volbu **Stav mostu**.

    g) V rozevírací nabídce **Typ prostředku**vyberte volbu **MQ-created Platform Events**.

    h) V rozevírací nabídce **Prvek prostředku**vyberte volbu **Celkem MQ-vytvořené události platformy**.

    i) Klepněte na tlačítko **Uložit**.

    Nakonfigurovali jste IBM MQ Console pro zobrazení celkového počtu IBM MQ vytvořených událostí platformy. Když je most spuštěn a začnete vkládat zprávy do tématu `/sf/mqtosfb/event/`*`Salesforce Platform Object Name/API name`* , modul widget zobrazí celkový počet událostí zpráv, které most vytvořil.

Deprecated Formát zprávy a chybové zprávy pro IBM MQ Bridge to Salesforce

Informace o formátování zpráv, které jsou zpracovány produktem IBM MQ Bridge to Salesforce.

Aplikace vloží zprávu do specifického tématu správce front, například `/`*`root`*`/mqtosfb/event/MQPlatformEvent1__e`. Most odebírá téma, získává obsah ze zpráv a používá jej k publikování zpráv událostí pro událost platformy Salesforce .

Musíte vytvořit událost platformy v produktu Salesforce a definovat pole obsahu, než budete moci použít most k vytvoření zpráv události pro tuto událost platformy. Název události platformy a její obsah určují, jak je třeba formátovat zprávu IBM MQ zpracovanou mostem. Pokud je například vaše Salesforce událost platformy **Object name** *MQPlatformEvent1* a vaše dvě vlastní definovaná pole jsou textová pole s **API name** *MyText__c* a *Name__c*, pak vaše zpráva IBM MQ , která je publikována v tématu `/root/mqtosfb/event/MQPlatformEvent1__e` , musí být ve správném formátu JSON:

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

Zprávy, které most spotřebovává a vytváří, jsou textové zprávy (MQSTR) ve formátu JSON. Vstupní zpráva je jednoduchý formát JSON a programy mohou ke generování použít zřetězení řetězců.

Chybové zprávy

Most může detekovat chyby, například pokud zpráva není v textovém formátu nebo Salesforce, například pokud název události platformy neexistuje. Pokud dojde k chybě při zpracování vstupní zprávy, zpráva se přesune do fronty chyb mostu spolu s vlastnostmi, které popisují chybu. Chyba je také zapsána do proudu *stderr* pro most.

Chyby generované produktem Salesforce jsou JSON. Níže jsou uvedeny některé chyby, které jsou způsobeny nesprávně formátovanými zprávami:

Chybný obsah události platformy, stav 400 Text

```
[{"message":"No such column 'Name__c' on sobject of type
MQPlatformEvent2__e","errorCode":"INVALID_FIELD"}
```

Neplatný název události platformy, text stavu 404

```
{"errorCode":"NOT_FOUND","message":"The requested resource does not exist"}
```

Chybný formát JSON, text stavu 400

```
{"errorCode":"NOT_FOUND","message":"The requested resource does not exist"}
```

Zpráva není JSON, text stavu 400

```
[{"message":
  "Unexpected character ('h' (code 104)): expected a valid value (number, String, array,
object, 'true', 'false' or 'null') at [line:1, column:2]",
  "errorCode":"JSON_PARSER_ERROR"}
```

Nejedná se o textovou zprávu (není odesláno na adresu Salesforce)

```
Error: Publication on topic ' /sf/mqtosfb/event/MQPlatformEvent1' does not contain a text
formatted message
```

Deprecated Linux Spuštění prostředí IBM MQ Bridge to Salesforce

Spusťte IBM MQ Bridge to Salesforce pro připojení k Salesforce a IBM MQ. Po připojení může most vytvářet odběry témat produktu Salesforce a znovu publikovat zprávy v tématu IBM MQ . Most může také vytvářet zprávy událostí pro události platformy Salesforce .

Než začnete

Dokončili jste kroky konfigurace v úloze :

- “Konfigurace agenta IBM MQ Bridge to Salesforce” na stránce 833
- “Vytvoření zpráv událostí pro události platformy Salesforce” na stránce 840

.

Informace o této úloze

Ke spuštění úlohy IBM MQ Bridge to Salesforcepoužijte konfigurační soubor, který jste vytvořili v předchozí úloze. Pokud jste nezahrnuli všechny požadované parametry do svého konfiguračního souboru, ujistěte se, že jste je zahrnuli do příkazového řádku.

Postup

1. Definujte témata typu push nebo události platformy v produktu Salesforce , pro které se chcete přihlásit k odběru produktu , nebo událost platformy, pro kterou chcete vytvořit zprávy události.
2. Spuštěním příkazu IBM MQ Bridge to Salesforce se připojte k produktu Salesforce a k vašemu správci front. Pokud spouštíte most pro odběr událostí produktu Salesforce , zadejte název tématu odeslání typu push nebo události platformy, které jste definovali v kroku 1.

   ```
   runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName
   ```

   Po připojení mostu jsou vráceny následující zprávy:

   - Používáte-li most k přihlášení k odběru událostí tématu odeslání typu push a platformy Salesforce :

     ```
     Successful connection to queue manager QM1
     Warning: Subscribing to MQ-created platform events is not enabled.
     Successful login to Salesforce at https://eu11.salesforce.com
     Ready to process events.
     ```

   - Pokud používáte most k vytváření zpráv událostí pro události platformy Salesforce :

     ```
     Successful connection to queue manager QM1
     Successful login to Salesforce at https://eu11.salesforce.com
     Successful subscription to '/sf/mqtosfb/event/+' for MQ-created platform events
     Ready to process events.
     ```

3. Volitelné: Odstraňte problémy s připojením ke správci front a k produktu Salesforce , pokud zprávy vrácené po spuštění mostu indikují, že připojení nebylo úspěšné.
   a) Zadejte příkaz v režimu ladění s volbou ladění 1.

      ```
      runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName -d 1
      ```

      Most prochází nastaveným připojením a zobrazuje zprávy o zpracování v režimu "terse".
   b) Zadejte příkaz v režimu ladění s volbou ladění 2.

      ```
      runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName -d 2
      ```

      Most prochází nastaveným připojením a zobrazuje zprávy zpracování v režimu s komentářem. Úplný výstup je zapsán do vašeho souboru protokolu.
4. Generujte události pomocí rozhraní Salesforce pro úpravu záznamů v databázi.
5. Přejděte do adresáře IBM MQ Console , abyste viděli změny témat odeslání typu push, které se objevují v modulu widget, který jste nakonfigurovali v předchozí úloze.

Jak pokračovat dále

Pomocí proměnné *MQSFB_EXTRA_JAVA_OPTIONS* můžete předat vlastnosti prostředí JVM, například chcete-li povolit trasování IBM MQ . Další informace viz Trasování IBM MQ Bridge to Salesforce.

Související úlohy

Monitorování produktu IBM MQ Bridge to Salesforce

Související odkazy

runmqsfb (spusťte příkaz IBM MQ Bridge to Salesforce)

Deprecated Linux z/OS MQ Adv. Konfigurace produktu IBM MQ pro použití s technologií blockchain

Nastavte a spusťte agenta IBM MQ Bridge to blockchain , abyste bezpečně připojili správce front IBM MQ Advanced nebo IBM MQ Advanced for z/OS Value Unit Edition a IBM Blockchain. Použijte most k asynchronnímu připojení, vyhledání a aktualizaci stavu prostředku v blockchainu pomocí aplikace systému zpráv, která se připojuje ke správci front IBM MQ Advanced nebo IBM MQ Advanced for z/OS VUE .

Než začnete

Notes:

- Deprecated Produkt IBM MQ Bridge to blockchain je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-341). Blockchain konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.
- Removed V 9.3.2 Pro Continuous Deliveryse IBM MQ Bridge to blockchain odebere z produktu na adrese IBM MQ 9.3.2.
- LTS IBM zamýšlí odebrat schopnost z vydání Long Term Support v nadcházejících opravných sadách. Máte-li aplikace, které budou touto změnou ovlivněny, obraťte se na podporu IBM .

  Upozornění: IBM MQ Bridge to blockchain built on Hyperledger Composer již není podporován.

  Chcete-li použít IBM MQ Bridge to blockchain vestavěný Hyperledger Fabric, musíte spustit produkt IBM MQ 9.1.4 nebo novější.
- Produkt IBM MQ Bridge to blockchain je k dispozici pouze pro připojení k následujícím správcům front:
  - Linux IBM MQ Advancednebo
  - z/OS IBM MQ Advanced for z/OS VUE
- Správce front musí mít stejnou úroveň příkazu jako most nebo vyšší; například IBM MQ 9.3.0.
- Produkt IBM MQ Bridge to blockchain je podporován pro použití s vaší blockchainovou sítí, která je založena na architektuře Hyperledger Fabric 1.4 .

Informace o této úloze

Blockchain je sdílená, distribuovaná, digitální transakční kniha, která se skládá z řetězce bloků, které představují dohodnuté transakce mezi rovnocennými partnery v síti. Každý blok v řetězci je propojen s předchozím blokem atd. zpět k první transakci.

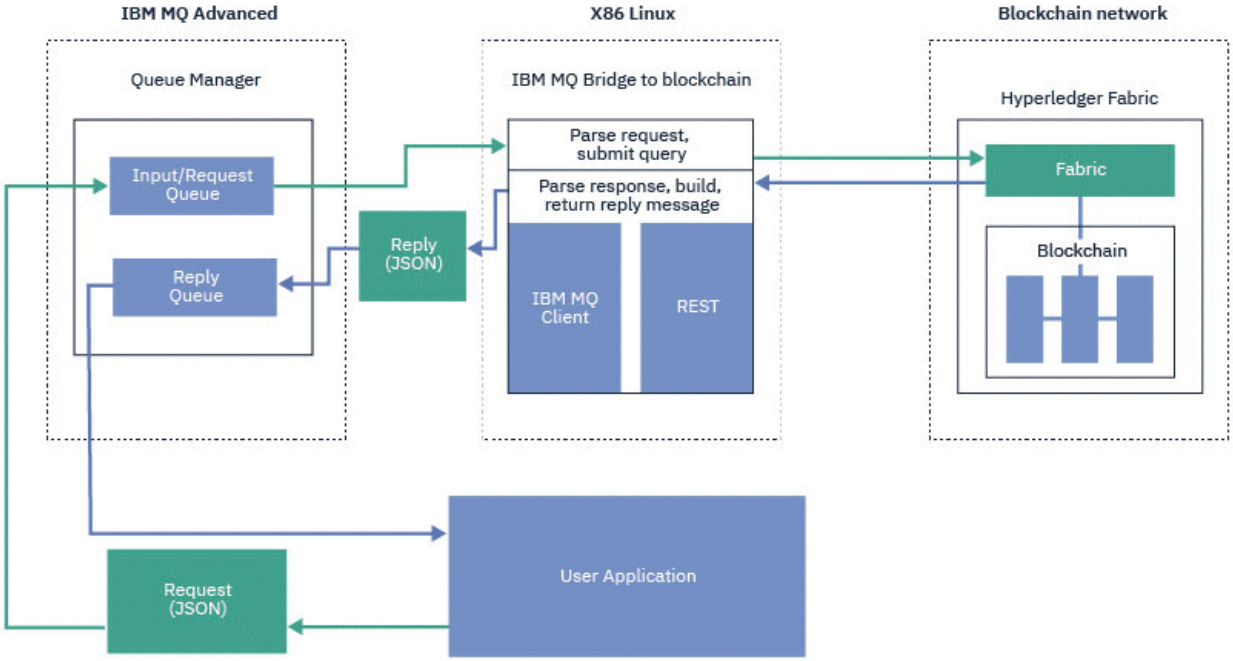
Produkt IBM Blockchain je postaven na produktu Hyperledger Fabric a můžete s ním vyvíjet lokálně pomocí produktu Docker nebo v kontejnerovém klastru v produktu IBM Cloud. Můžete také aktivovat a používat svou síť IBM Blockchain v produkčním prostředí, vytvářet a řídit obchodní síť s vysokou úrovní zabezpečení, soukromí a výkonu. Další informace viz IBM Blockchain Platform.

Hyperledger Fabric je open source, podnikový blockchain framework, který je vyvíjen ve spolupráci členy Hyperledger Project, včetně IBM jako počáteční přispěvatel kódu. Hyperledger Project, nebo Hyperledger, je Linux Foundation open source, globální iniciativa pro spolupráci, která má pokročit v technologiích blockchainu napříč odvětvovými odvětvovými odvětvovými odvětvovými odvětvovými technologiemi. Další informace viz IBM Blockchain, Hyperledger Projektya Hyperledger Fabric.

Pokud již používáte IBM MQ Advancednebo IBM MQ Advanced for z/OS VUEa IBM Blockchain, můžete použít IBM MQ Bridge to blockchain k odesílání jednoduchých dotazů, aktualizací a přijímání odpovědí ze své blockchainové sítě. Tímto způsobem můžete integrovat místní software IBM s cloudovou službou blockchain.

Stručný přehled provozního procesu mostu naleznete na obrázku 1. Uživatelská aplikace vloží zprávu ve formátu JSON do fronty vstupu/požadavku ve správci front IBM MQ Advancednebo IBM MQ Advanced

for z/OS VUE . Most se připojí ke správci front, získá zprávu z fronty vstupů/požadavků, zkontroluje, zda je formát JSON správně naformátován, a poté vydá dotaz nebo aktualizaci blockchainu. Data vrácená technologií blockchain jsou analyzována mostem a umístěna do fronty odpovědí, jak je definováno v původní zprávě požadavku IBM MQ . Uživatelská aplikace se může připojit ke správci front, načíst zprávu odpovědi z fronty odpovědí a použít informace.



Obrázek 98. IBM MQ Bridge to blockchain

Produkt IBM MQ Bridge to blockchain můžete nakonfigurovat tak, aby se připojil k síti blockchainu jako účastník nebo jako partner. Je-li most spuštěn, aplikace systému zpráv požádá most o řízení rutin řetězového kódu, které se dotazují nebo aktualizují stav prostředku a vracejí výsledky jako odezvu do aplikace systému zpráv.

Postup

1. Vytvořte a spusťte správce front nebo spusťte existujícího správce front, kterého chcete použít se svým produktem IBM MQ Bridge to blockchain.

   Vytvořit správce front:

   ```
   crtmqm adv_qmgr_name
   ```

   Spustit správce front:

   ```
   strmqm adv_qmgr_name
   ```

2. Vytvořte fronty pro most, které jsou definovány ve skriptu **DefineQ.mqsc** .

   Pro výchozí pojmenované fronty, které se používají pro:

   - Pověření uživatele, například `SYSTEM.BLOCKCHAIN.IDENTITY.QUEUE`
   - Vstup zprávy do mostu, například `APPL1.BLOCKCHAIN.INPUT.QUEUE`
   - Odpovědi z blockchainu, například `APPL1.BLOCKCHAIN.REPLY.QUEUE`

   V adresáři `/opt/mqm/mqbc/samp` zadejte následující příkaz:

   ```
   runmqsc adv_qmgr_name < ./DefineQ.mqsc
   ```

Různé aplikace mohou používat stejnou vstupní frontu, ale můžete zadat více front odpovědí, jednu pro každou z vašich aplikací. Nemusíte používat definované fronty odpovědí. Chcete-li pro odpovědi použít dynamické fronty, musíte zvážit jejich konfiguraci zabezpečení.

Výsledky

Vytvořili jste fronty, které most vyžaduje pro zpracování zpráv z produktu IBM MQ a vaší blockchainové sítě.

Jak pokračovat dále

Použijte informace o správci front IBM MQ Advancednebo IBM MQ Advanced for z/OS VUEa pověření ze sítě blockchain k vytvoření konfiguračního souboru pro IBM MQ Bridge to blockchain.

Deprecated Vytvoření konfiguračního souboru pro IBM MQ Bridge to blockchain

Zadejte správce front a parametry sítě blockchain, abyste vytvořili konfigurační soubor pro IBM MQ Bridge to blockchain pro připojení k sítím IBM MQ a IBM Blockchain .

Než začnete

- Vytvořili jste a nakonfigurovali síť blockchain.
- Máte soubor pověření ze sítě blockchain.
- Nainstalovali jste produkt IBM MQ Bridge to blockchaindo svého prostředí x86 Linux .

  Další informace naleznete v tématu Instalace serveru IBM MQ na systémech Linux a IBM MQ komponenty rpm pro systémy Linux.
- Spustili jste správce front IBM MQ Advanced .

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným pro vytvoření konfiguračního souboru IBM MQ Bridge to blockchain a úspěšné připojení k sítím IBM Blockchain a IBM MQ .

Most můžete použít pro připojení k sítím blockchainu, které jsou založeny na Hyperledger Fabric 1.4 architecture. Chcete-li použít most, potřebujete informace o konfiguraci ze sítě blockchain. V každém kroku této úlohy najdete příklad podrobností konfigurace, které jsou založeny na dvou různě nakonfigurovaných sítích blockchain:

- Hyperledger Fabric síť, která běží v Docker. Další informace viz téma Začínáme s produktem Hyperledger Fabric, Psaní první aplikacea “Příklad souboru pověření sítě Hyperledger Fabric” na stránce 851.
- Hyperledger Fabric síť, která běží v Kubernetes klastru v IBM Cloud. Další informace viz téma Vývoj v cloudovém sandboxu na platformě IBM Blockchain Platform.

Postup

1. Spusťte most a vytvořte konfigurační soubor.

   Potřebujete parametry ze souboru pověření sítě blockchain a ze správce front IBM MQ Advanced .

   ```
   runmqbcb -o config_file_name.cfg
   ```

   Jak ukazuje následující příklad, existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte klávesu `Enter` , abyste přijali existující hodnoty, stiskněte klávesu `Space` a poté `Enter` , abyste vymazali hodnoty, a zapište do hranatých závorek, pak stiskněte klávesu `Enter` , abyste přidali nové hodnoty. Seznamy hodnot (například rovnocenných hodnot) můžete oddělit čárkami nebo zadáním každé hodnoty na nový řádek. Seznam končí prázdným řádkem.

   Poznámka: Existující hodnoty nelze upravit. Můžete je zachovat, nahradit nebo vymazat.

2. Zadejte hodnoty pro připojení ke správci front IBM MQ Advanced .

   Minimální hodnoty potřebné pro připojení jsou název správce front, názvy vstupních front mostu a fronty identit, které jste definovali. Pro připojení ke vzdáleným správcům front potřebujete také **MQ Channel** a **MQ Conname** (adresa hostitele a port, kde je spuštěn správce front). Chcete-li použít TLS pro připojení k IBM MQ v kroku “4” na stránce 851, musíte použít rozhraní JNDI nebo CCDT a odpovídajícím způsobem zadat **MQ CCDT URL** nebo **JNDI implementation class** a **JNDI provider URL** .
3. 13. Zadejte pověření serveru Hyperledger Fabric pro vaši síť.

   Příklady toho, co byste měli očekávat, jsou uvedeny v následujícím kódu:

```
Fabric Server
--------------
Network configuration file          : []connection-tls.json
Wallet                              : []
User Name                           : []User1
Certificate                         : []<path_to_user_certificate>
Private Key                         : []<path_to_private_key>/private_key.pem
Organisation                        : []Org1MSP
```

4. Zadejte hodnoty úložiště certifikátů pro připojení TLS.

   Ponechte tuto oblast prázdnou, pokud ji nemáte.

```
Certificate stores for MQ TLS connections
-----------------------------------------
Personal keystore                   : []
Keystore password                   : []
Trusted store for signer certs      : []
Trusted store password              : []
```

5. Zadejte cestu k souboru protokolu, do kterého mají být zapisovány protokoly mostu.

```
Behavior of bridge program
--------------------------
Runtime logfile for copy of stdout/stderr : []bridgelog.log
Number of logfiles                  : [3]
Maximum size of each logfile (bytes) : [2097152]
```

Upozornění: Dříve byly v tomto nastavení mostu uloženy podrobnosti týkající se modulu Peers, Orderers a certifikační autority. Tyto informace jsou však nyní uloženy v *konfiguračním souboru sítě*, který je propojen v části nastavení serveru Hyperledger Fabric .

Výsledky

Vytvořili jste konfigurační soubor, který produkt IBM MQ Bridge to blockchain používá pro připojení k síti IBM Blockchain a ke správci front IBM MQ Advanced .

Jak pokračovat dále

Projděte kroky pro “Spuštění prostředí IBM MQ Bridge to blockchain” na stránce 855.

Deprecated Příklad souboru pověření sítě Hyperledger Fabric

Obsah souboru `.yml` z lokálně převedené sítě Hyperledger Fabric blockchain spuštěné v produktu Docker, který můžete použít ke konfiguraci serveru IBM MQ Bridge to blockchain.

IBM MQ Bridge to blockchain je k dispozici pro připojení k:

- Linux IBM MQ Advancednebo
- z/OS IBM MQ Advanced for z/OS VUE

pouze správci front.

Poté, co jste prošli výukovými programy Začínáme s produktem Hyperledger Fabric , porozuměli Co se děje v zákulisía spustili síť pomocí jednoho z Hyperledger Fabric ukázek, měli byste mít ve složce / `blockchain/fabric-samples/basic-network` následující konfigurační soubor.

Chcete-li se připojit k síti blockchain, musíte použít podrobnosti konfigurace z tohoto souboru, když jste “Vytvoření konfiguračního souboru pro IBM MQ Bridge to blockchain” na stránce 850.

```
{
  "name": "basic-network",
  "version": "1.0.0",
  "client": {
    "organization": "Org1",
    "connection": {
      "timeout": {
        "peer": {
          "endorser": "300"
        },
        "orderer": "300"
      }
    }
  },
  "channels": {
    "mychannel": {
      "orderers": [
        "orderer.example.com"
      ],
      "peers": {
        "peer0.org1.example.com": {
          "endorsingPeer": true,
          "chaincodeQuery": true,
          "ledgerQuery": true,
          "eventSource": true
        },
        "peer0.org2.example.com": {
          "endorsingPeer": true,
          "chaincodeQuery": false,
          "ledgerQuery": true,
          "eventSource": false
        }
      }
    }
  },
  "organizations": {
    "Org1": {
      "mspid": "Org1MSP",
      "peers": [
        "peer0.org1.example.com"
      ],
      "certificateAuthorities": [
        "ca-org1"
      ],
      "adminPrivateKeyPEM": {
        "path": "$<path_to_private_key>/admin_private_key"
      },
      "signedCertPEM": {
        "path": "<path_to_org_signed_cert>/Admin@org1.example.com-cert.pem"
      }
    },
    "Org2": {
      "mspid": "Org2MSP",
      "peers": [
        "peer0.org2.example.com"
      ],
      "certificateAuthorities": [
        "ca-org2"
      ]
    }
  },
  "orderers": {
    "orderer.example.com": {
      "url": "grpcs://localhost:7050",
      "mspid": "OrdererMSP",
      "grpcOptions": {
        "ssl-target-name-override": "orderer.example.com",
        "hostnameOverride": "orderer.example.com"
      },
      "tlsCACerts": {
        "path": "<path_to_orderer_cert>/ca.crt"
```

```
      },
      "adminPrivateKeyPEM": {
        "path": <path_to_orderers_private_key>/<private_key>"
      },
      "signedCertPEM": {
        "path": "<path_to_orderer_signed_cert>/Admin@example.com-cert.pem"
      }
    }
  },
  "peers": {
    "peer0.org1.example.com": {
      "url": "grpcs://localhost:7051",
      "grpcOptions": {
        "ssl-target-name-override": "peer0.org1.example.com",
        "hostnameOverride": "peer0.org1.example.com",
        "request-timeout": 120001
      },
      "tlsCACerts": {
        "path": <path_to_peer_cert>/ca.crt"
      }
    },
    "peer0.org2.example.com": {
      "url": "grpcs://localhost:9051",
      "grpcOptions": {
        "ssl-target-name-override": "peer0.org2.example.com",
        "hostnameOverride": "peer0.org2.example.com",
        "request-timeout": 120001
      },
      "tlsCACerts": {
        "path": "<path_to_peer_cert>/ca.crt"
      }
    }
  },
  "certificateAuthorities": {
    "ca-org1": {
      "url": "https://localhost:7054",
      "grpcOptions": {
        "verify": true
      },
      "tlsCACerts": {
        "path": "<path_to_ca_cert>/ca.org1.example.com-cert.pem"
      },
      "registrar": [
        {
          "enrollId": "admin",
          "enrollSecret": "adminpw"
        }
      ]
    },
    "ca-org2": {
      "url": "https://localhost:8054",
      "grpcOptions": {
        "verify": true
      },
      "tlsCACerts": {
        "path": "<path_to_ca_cert>/ca.org2.example.com-cert.pem"
      },
      "registrar": [
        {
          "enrollId": "admin",
          "enrollSecret": "adminpw"
        }
      ]
    }
  }
}
```

Deprecated Linux Formáty zpráv pro IBM MQ Bridge to blockchain z IBM MQ 9.2.0

Informace o formátování zpráv, které jsou odesílány a přijímány produktem IBM MQ Bridge to blockchain.

Aplikace požaduje, aby produkt IBM MQ Bridge to blockchain řídil server Hyperledger Fabric , aby jednal s informacemi, které jsou zadrženy na blockchainu. Aplikace to provede umístěním zprávy požadavku do fronty požadavků mostu. Výsledky požadavku jsou zformátovány mostem do zprávy odpovědi. Most

používá informace obsažené v polích **ReplyToQ** a **ReplyToQMgr** z deskriptoru MQMD zprávy požadavku jako místo určení pro zprávu odpovědi.

Zprávy požadavků a odpovědí jsou textové zprávy (MQSTR) ve formátu JSON a obsahují čtyři prvky.

Formát zprávy požadavku

Zprávy požadavků obsahují následující atributy:

Operace
Bez rozlišování velkých a malých písmen

`submit` pro aktualizace nebo `evaluate` pro dotazy

síť
Řetězec-někdy označovaný jako `channel` v Hyperledger Fabric

Smlouva.
Řetězec-inteligentní smlouva nebo balík řetězcového kódu, který má být vyvolán

argumenty
Pole-obvykle řetězců, ale některé prvky mohou být vnořené objekty JSON.

Skutečné argumenty pro **`contract`**, včetně názvu metody.

Příklad:

```
{
  "operation" : "Evaluate",
  "network"   : "mychannel",
  "contract"  : "marbles0",
  "args"      : [ "readMarble" , "marble1" ]
}
```

Poznámka: Kromě toho, že se ujistíte, že tyto prvky existují a že zpráva je platný formát JSON, most neprovede žádné ověření obsahu. Most spoléhá na to, že produkt Hyperledger Fabric zpracuje požadavek nebo vrátí chyby.

Formát zprávy odpovědi

Zprávy odpovědí mají své ID korelace nastaveno na ID zprávy příchozí zprávy. Všechny vlastnosti definované uživatelem se zkopírují ze zprávy požadavku do zprávy odpovědi. ID uživatele v odpovědi je nastaveno na ID uživatele původce.

`statusCode` je stavový kód HTTP . Pokud je chyba z IBM MQ nebo mostu, použije se odpovídající hodnota **`statusCode`** .

`statusType` je řetězec, buď *ÚSPĚCH* , nebo *SELHÁNÍ*.

V případě úspěšných požadavků obsahuje prvek "**`data`**" ve zprávě odpovědi odezvu z vyvolaného rozhraní Hyperledger Composer REST API.

Příklad úspěšného zpracování:

```
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "data": [
      {
         "$class": "org.example.trading",
         "firstName": "John",
         "lastName": "Doe",
         "tradeId": "Trader1"
      },
      {
         "$class": "org.example.trading",
         "firstName": "Jane",
         "lastName": "Doe",
         "tradeId": "Trader2"
      }
```

```
   ]
}
```

Všechny chybové odpovědi mají stejná pole, bez ohledu na to, zda jsou generovány samotným mostem, z volání na server Hyperledger Composer REST, blockchain nebo z vyvolání řetězového kódu. Příklad:

- Chybná vstupní zpráva JSON

```
{
   "statusCode": 400,
   "statusType": "FAILURE",
   "message": "[AMQBC021E] Error: Cannot parse input message or there are
    missing fields in the message. Missing fields appear to be: "method"."
}
```

- Požadavek, který se nepodařilo zpracovat serverem Hyperledger Composer REST

```
{
   "statusCode": 500,
   "statusType": "FAILURE",
   "message": "Error trying to invoke business network. Error: No valid responses
    from any peers.\nResponse from attempted peer comms was an error: Error: chaincode
    error (status: 500, message: Error: Failed to add object with ID 'Trader1'
    as the object already exists)"
}
```

Aplikace mohou určit, zda byl požadavek úspěšný nebo selhal, buď pohledem na řetězec **statusType** , nebo z existence datového pole. Pokud dojde k chybě při zpracování vstupní zprávy a most ji neodešle do blockchainu, hodnota vrácená z mostu je hodnota MQRC, obvykle **MQRC_FORMAT_ERROR**.

Deprecated Spuštění prostředí IBM MQ Bridge to blockchain

Spusťte IBM MQ Bridge to blockchain pro připojení k IBM Blockchain a IBM MQ. Po připojení je most připraven zpracovat zprávy požadavků, odeslat je do sítě blockchainu Hyperledger Composer a přijmout a zpracovat odpovědi.

Informace o této úloze

Ke spuštění úlohy IBM MQ Bridge to blockchainpoužijte konfigurační soubor, který jste vytvořili v předchozí úloze.

Postup

1. Spusťte správce front IBM MQ Advanced , kterého chcete použít s mostem.
2. Spuštěním rozhraní IBM MQ Bridge to blockchain se připojte k serveru Hyperledger Composer REST a ke správci front IBM MQ Advanced .

   Spusťte příkaz mostu.

   ```
   runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
   ```

   Je-li most připojen, je vrácen výstup podobný následujícímu:

   ```
   2018-05-17 14:28:16.866 BST IBM MQ Bridge to Blockchain
   5724-H72 (C) Copyright IBM Corp. 2017, 2024.

   2018-05-17 14:28:19.331 BST Ready to process input messages.
   ```

3. Volitelné: Odstraňte problémy s připojením ke správci front IBM MQ Advanced a k síti blockchain, pokud zprávy vrácené po spuštění mostu indikují, že připojení není úspěšné.

   a) Zadejte příkaz v režimu ladění s volbou ladění 1.

```
runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
-d 1
```

Most prochází nastaveným připojením a zobrazuje zprávy o zpracování v režimu "terse".

b) Zadejte příkaz v režimu ladění s volbou ladění 2.

```
runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
-d 2
```

Most prochází nastaveným připojením a zobrazuje zprávy zpracování v režimu s komentářem. Úplný výstup je zapsán do vašeho souboru protokolu.

Výsledky

Spustili jste produkt IBM MQ Bridge to blockchain a připojili jste se ke správci front a síti blockchain pomocí serveru Hyperledger Composer REST.

Jak pokračovat dále

- Chcete-li formátovat a odeslat dotaz nebo zprávu o aktualizaci do sítě blockchain, postupujte podle pokynů v části “Spuštění ukázky klienta IBM MQ Bridge to blockchain v systému z/OS” na stránce 858 .
- Použijte proměnnou *MQBCB_EXTRA_JAVA_OPTIONS* k předání vlastností prostředí JVM, například k povolení trasování IBM MQ . Další informace viz Trasování IBM MQ Bridge to blockchain.

Deprecated z/OS Formáty zpráv pro IBM MQ Bridge to blockchain před IBM MQ 9.2.0 na z/OS

Informace o formátování zpráv, které jsou odesílány a přijímány produktem IBM MQ Bridge to blockchain.

Upozornění: Existující formát pro formáty zpráv je zastaralý. V systému IBM MQ 9.2.0, pokud máte síť Hyperledger Fabric , použijte formát zpráv popsaných v části “Formáty zpráv pro IBM MQ Bridge to blockchain z IBM MQ 9.2.0” na stránce 853.

Aplikace požaduje, aby produkt IBM MQ Bridge to blockchain řídil rozhraní REST API definované produktem Hyperledger Composer , aby jednal s informacemi, které jsou zadrženy na blockchainu. Aplikace to provede umístěním zprávy požadavku do fronty požadavků mostu. Výsledky požadavku REST jsou zformátovány mostem do zprávy odpovědi. Most používá informace obsažené v polích **ReplyToQ** a **ReplyToQMgr** z deskriptoru MQMD zprávy požadavku jako místo určení pro zprávu odpovědi.

Zprávy požadavku a odpovědi jsou textové zprávy (MQSTR) ve formátu JSON.

Formát zprávy požadavku

Zprávy požadavků obsahují tři atributy:

metoda
Příkaz REST použitý k volání rozhraní REST API produktu Hyperledger Composer , jako např. POST, DELETE nebo GET

cesta
Cesta k rozhraní Hyperledger Composer REST API. Toto se přidá na základní server URL. Cesta by měla začínat na "`api/`".

tělo
Obsah specifický pro danou metodu. Toto je často struktura JSON.

Následující příklad používá metodu POST pro cestu `api/Traderk` vytvoření nového objektu Trader. Tělo specifikuje třídu Traders, jak je definována v modelu Hyperledger Composer uživatele, a také specifikuje další hodnoty potřebné k vytvoření nového objektu Trader v rámci blockchainové sítě.

```
{ "method": "POST",
  "path": "api/Trader",
```

```
  "body": {
    "$class" : "org.example.trading",
    "tradeId" : "Trader2",
    "firstName": "Jane",
    "lastName" : "Doe"
```

Formát zprávy odpovědi

Zprávy odpovědí mají své ID korelace nastaveno na ID zprávy příchozí zprávy. Všechny vlastnosti definované uživatelem se zkopírují ze zprávy požadavku do zprávy odpovědi. ID uživatele v odpovědi je nastaveno na ID uživatele původce.

statusCode je stavový kód HTTP . Pokud je chyba z IBM MQ nebo mostu, použije se odpovídající hodnota **statusCode** .

statusType je řetězec, buď *ÚSPĚCH* , nebo *SELHÁNÍ*.

V případě úspěšných požadavků obsahuje prvek "**data**" ve zprávě odpovědi odezvu z vyvolaného rozhraní Hyperledger Composer REST API.

Příklad úspěšného zpracování:

```
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "data": [
      {
         "$class": "org.example.trading",
         "firstName": "John",
         "lastName": "Doe",
         "tradeId": "Trader1"
      },
      {
         "$class": "org.example.trading",
         "firstName": "Jane",
         "lastName": "Doe",
         "tradeId": "Trader2"
      }
   ]
}
```

Všechny chybové odpovědi mají stejná pole, bez ohledu na to, zda jsou generovány samotným mostem, z volání na server Hyperledger Composer REST, blockchain nebo z vyvolání řetězového kódu. Příklad:

- Chybná vstupní zpráva JSON

```
{
   "statusCode": 400,
   "statusType": "FAILURE",
   "message": "[AMQBC021E] Error: Cannot parse input message or there are
    missing fields in the message. Missing fields appear to be: "method"."
}
```

- Požadavek, který se nepodařilo zpracovat serverem Hyperledger Composer REST

```
{
   "statusCode": 500,
   "statusType": "FAILURE",
   "message": "Error trying to invoke business network. Error: No valid responses
    from any peers.\nResponse from attempted peer comms was an error: Error: chaincode
    error (status: 500, message: Error: Failed to add object with ID 'Trader1'
    as the object already exists)"
}
```

Aplikace mohou určit, zda byl požadavek úspěšný nebo selhal, buď pohledem na řetězec **statusType** , nebo z existence datového pole. Pokud dojde k chybě při zpracování vstupní zprávy a most ji neodešle do blockchainu, hodnota vrácená z mostu je hodnota MQRC, obvykle **MQRC_FORMAT_ERROR**.

Deprecated z/OS Spuštění ukázky klienta IBM MQ Bridge to blockchain v systému z/OS

Pomocí ukázky klienta JMS , která je součástí produktu IBM MQ Bridge to blockchain, můžete vložit zprávu do vstupní fronty, kterou most blockchain kontroluje, a zobrazit přijatou odpověď. Tato ukázka je založena na použití produktu IBM MQ Bridge to blockchain , který je integrován s příkladem sítě Hyperledger Composer Trader.

Než začnete

Další informace viz /trade_network

Produkt IBM MQ Bridge to blockchain je spuštěn a je připojen ke správci front IBM MQ Advanced nebo IBM MQ Advanced for z/OS VUE a k síti blockchain.

Informace o této úloze

Vyhledejte ukázkovou aplikaci JMS (`ComposerBCBSamp.java`) v adresáři `samp` v souboru IBM MQ Bridge to blockchain.

Například: `<MQ_INSTALL_ROOT>/mqbc/samp/ComposerBCBSamp.java`, kde `<MQ_INSTALL_ROOT>` je:

- Linux Adresář, kde je nainstalován produkt IBM MQ
- z/OS Adresář z/OS UNIX System Services , kde jsou nainstalovány komponenty z/OS UNIX produktu IBM MQ

.

Postup

1. Upravte ukázkový zdrojový soubor Java klienta.

   Postupujte podle pokynů v ukázce a nakonfigurujte jej tak, aby odpovídal vašemu prostředí IBM MQ a vaší blockchainové síti.

   Následující kód z ukázky definuje tři zprávy požadavku JSON, které se mají odeslat na most:

   a. Za prvé, odstranit existující '`commodity`'

   b. Za druhé, chcete-li vytvořit nové '`commodity`', '`owner`' a přidružené hodnoty,

   c. Nakonec zobrazí nové informace o '`commodity`' po předchozích dvou zprávách požadavku.

```
private static JSONObject[] createMessageBodies() {
    JSONObject[] msgs = new JSONObject[3]; // This method creates 3 messages
    JSONObject m, m2;
    String commodityName = "BC";

    // Clean out the commodity in case it's already there. If
    // it's not there, there will be an error returned from Composer.
    m = new JSONObject();
    m.put("method", "DELETE");
    m.put("path", "api/Commodity/" + commodityName);
    msgs[0] = m;

    // To add the item to the table, the
    // operation looks like this:
    //
    // { "method": "POST",
    //   "path": "api/Commodity",
    //   "body" : {
    //     "$class": "org.example.trading.Commodity",
    //     "tradingSymbol" : "BC",
    //     "description" : "BC",
    //     "mainExchange" : "HERE",
    //     "owner" : "Me",
```

```
    //     "quantity" : 100
    //   }
    // }
    // You can see this structure in the API Explorer
    m = new JSONObject();
    m.put("method", "POST");
    m.put("path", "api/Commodity");
    m2 = new JSONObject();
    m2.put("$class", " org.example.trading.Commodity");
    m2.put("tradingSymbol", commodityName);
    m2.put("description", "Blockchain Sample Description");
    m2.put("mainExchange", "My Exchange");
    m2.put("owner", "Me");
    m2.put("quantity", 100);
    m.put("body", m2);
    msgs[1] = m;

    // And list all items that have been created
    m = new JSONObject();
    m.put("method", "GET");
    m.put("path", "api/Commodity");
    msgs[2] = m;

    return msgs;
  }
```

2. Zkompilujte ukázku.

   Odkažte na třídy klienta IBM MQ a soubor JSON4J.jar , které jsou dodávány v adresáři mostu.

```
javac -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar
ComposerBCBClient.java
```

3. Spusťte kompilovanou třídu.

```
java -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar:.
ComposerBCBClient
```

```
Starting Simple MQ Blockchain Bridge Client
Starting the connection.
Sent message:
  {"method":"DELETE"," path ":"api\/Commodity\/BC"}
Response text:
{
   "statusCode": 204,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": ""
}
SUCCESS
Sent message:
{"body":
{"$class":"org.example.trading.Commodity","owner":"Me","quantity":100,"description":"Blockcha
in Sample Description","mainExchange":"My
Exchange","tradingSymbol":"BC"},"operation":"POST","url":"Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": {
      "$class": "org.example.trading.Commodity",
      "description": "Blockchain Sample Description",
      "mainExchange": "My Exchange",
      "owner": "Me",
      "quantity": 100,
      "tradingSymbol": "BC"
   }
}
SUCCESS
Sent message:
  {"method":"GET","path":"api\/Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
```

```
    "message": "OK",
    "data": [
       {
          "$class": "org.example.trading.Commodity",
          "description": "Blockchain Sample Description",
          "mainExchange": "My Exchange",
          "owner": "resource:org.example.trading.Trader#Me",
          "quantity": 100,
          "tradingSymbol": "BC"
       }
    ]
}
SUCCESS
```

Pole **message** obsahuje buď "OK" pro úspěšně zpracovanou zprávu, nebo v případě nezdařeného požadavku informace týkající se příčiny selhání.

Pokud klient obdrží chybu časového limitu při čekání na odezvu, zkontrolujte, zda je most spuštěn.

Deprecated Linux Další volby konfigurace pro IBM MQ Bridge to blockchain

Od produktu IBM MQ 9.2.0dochází ke změně způsobu, jakým trasování a protokolování funguje na systému IBM MQ Bridge to blockchain.

Změny z konzoly IBM MQ 9.1.0 IBM MQ Bridge to blockchain

Standardně nedochází k žádným změnám chování z mostu IBM MQ 9.1.0 , kromě souboru protokolu, který se nyní začíná otáčet. Další informace viz “Výměnné protokoly” na stránce 860.

Interakce trasování a ladění

V produktu IBM MQ 9.2.0se příznak ladění i nadále bude chovat jako v případě IBM MQ 9.1.0. To znamená, že *-d1* poskytuje informace o ladění mostu a *-d2* zapíná protokolování ladění pro nezbytné komponenty. Pokud jste však při spuštění mostu povolili trasování systému IBM MQ , bude vytváření sestav na úrovni *-d2* automaticky zapnuto.

Výměnné protokoly

V systému IBM MQ 9.2.0je výchozím chováním souboru protokolu tři soubory protokolu, každý o velikosti 2 MB. Tyto hodnoty můžete přepsat pomocí dalších vlastností konfigurace. Existující atribut konfigurace nebo parametr příkazového řádku pro soubor protokolu je považován za základní název protokolů s přidaným indexem.

Pokud má nakonfigurovaný soubor protokolu:

- Žádný typ souboru, index se přidá na konec názvu souboru.

  Nastavení souboru protokolu na hodnotu `abc`vede k protokolům s názvem `abc.0`, `abc.1`atd.

- Typ souboru, index je vložen před typ souboru.

  Nastavení souboru protokolu na hodnotu `abc.log`vede k protokolům s názvem `abc.0.log`, `abc.1.log`atd.

Notes:

1. Vzhledem k tomu, že mosty mohou být spuštěny s libovolným oprávněním uživatele, není možné vynutit určitý adresář, například `/var/mqm/qmgrs/<qm>/errors`, pro protokoly.
2. Stejné informace se i nadále zapisují do proudů *stdout* a *stderr* .
3. Při každém opětovném otevření jednotlivého souboru protokolu se znovu vytisknou základní informace o konfiguraci. Informace budou vždy k dispozici, místo aby byly vytištěny pouze jednou na začátku programu.

Deprecated z/OS MQ Adv. VUE Konfigurace produktu IBM MQ Advanced for z/OS VUE pro použití s technologií blockchain

Nastavte a spusťte agenta IBM MQ Bridge to blockchain , abyste zabezpečeně připojili agenta IBM MQ na z/OS správci front a IBM Blockchain. Most lze použít k asynchronnímu připojení, vyhledání a aktualizaci stavu prostředku v blockchainu pomocí aplikace systému zpráv, která se připojuje ke správci front produktu IBM MQ Advanced for z/OS VUE .

Než začnete

Notes:

- Deprecated Produkt IBM MQ Bridge to blockchain je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-341). Blockchain konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.
- Removed V 9.3.2 Pro Continuous Deliveryse IBM MQ Bridge to blockchain odebere z produktu na adrese IBM MQ 9.3.2.
- Produkt IBM MQ Bridge to blockchain je k dispozici jako součást balíku konektoru na systému IBM MQ Advanced for z/OS Value Unit Edition 9.1.0. Můžete se připojit ke správcům front IBM MQ Advanced for z/OS VUE , kteří jsou spuštěni na stejné úrovni příkazu nebo vyšší.
- Produkt IBM MQ Bridge to blockchain je podporován pro použití s vaší blockchainovou sítí, která je založena na Hyperledger Composer sestaveném Hyperledger Fabric.
- Produkt IBM MQ Bridge to blockchain musí být nainstalován v prostředí z/OS UNIX System Services a vyžaduje verzi 8 Java runtime environment z IBM.

Informace o této úloze

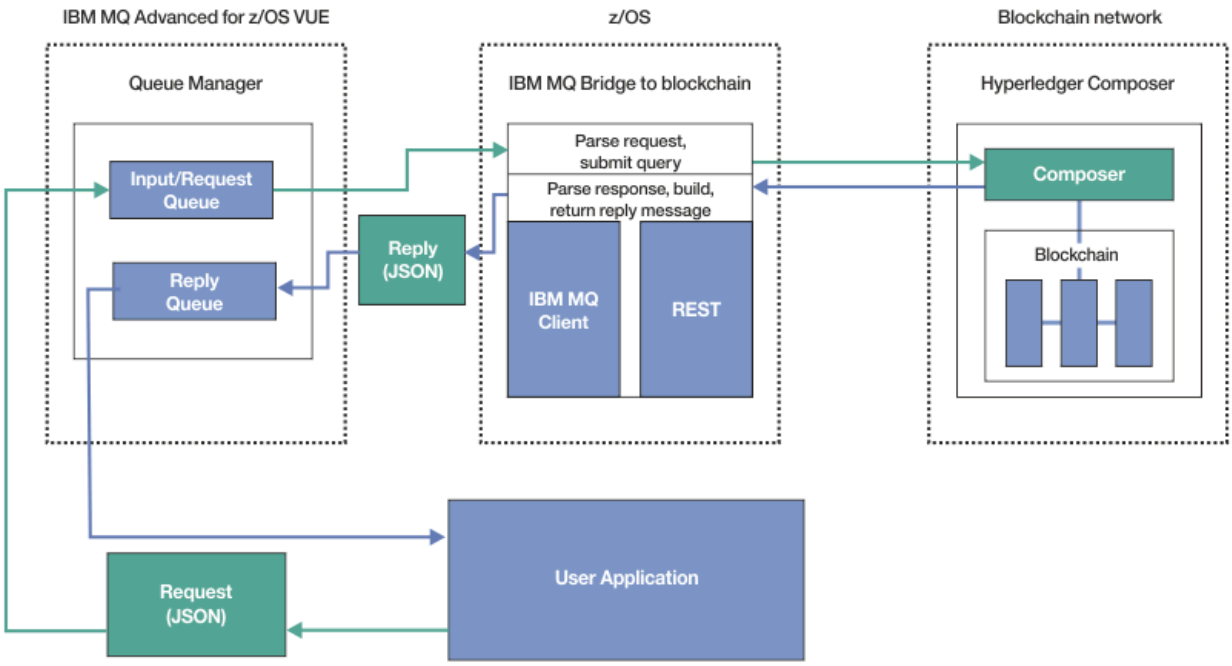
Blockchain je sdílená, distribuovaná, digitální transakční kniha, která se skládá z řetězce bloků, které představují dohodnuté transakce mezi rovnocennými partnery v síti. Každý blok v řetězci je propojen s předchozím blokem atd. zpět k první transakci.

Produkt IBM Blockchain je sestaven na systémech Hyperledger Fabric a Hyperledger Composer. Můžete s ním vyvíjet lokálně pomocí produktu Dockernebo v klastru kontejnerů v produktu IBM Cloud. Můžete také aktivovat a používat svou síť IBM Blockchain v produkčním prostředí, abyste vytvořili a řídili obchodní síť s vysokou úrovní zabezpečení, soukromí a výkonu. Další informace viz IBM Blockchain Platform.

Hyperledger Fabric a Hyperledger Composer jsou open source, podnikový rámec blockchain, který je vyvíjen ve spolupráci členy Hyperledger Project, včetně IBM jako počátečního přispěvatele kódu. Hyperledger Project, nebo Hyperledger, je Linux Foundation open source, globální iniciativa pro spolupráci, která má pokročit v technologiích blockchainu napříč odvětvovými odvětvovými odvětvovými odvětvovými odvětvovými technologiemi. Další informace viz IBM Blockchain, Hyperledger Projekty, Hyperledger Fabrica Hyperledger Composer.

Pokud již používáte IBM MQ Advanced for z/OS VUE a IBM Blockchain, můžete použít IBM MQ Bridge to blockchain k řízení svého obchodního modelu Hyperledger Composer přes rozhraní REST Hyperledger Composer , což vám umožní aktualizovat nebo dotazovat se na stav ve vašem blockchainu a přijímat odpovědi zpět z vaší blockchainové sítě. Tímto způsobem můžete integrovat místní software IBM buď s cloudovou službou blockchain, nebo lokálně spravovaným místním řešením.

Stručný přehled provozního procesu mostu je uveden na Obrázku 1. Uživatelská aplikace vloží zprávu ve formátu JSON do vstupní fronty/fronty požadavků ve správci front z/OS . Pomocí serveru Hyperledger Composer REST se most připojí ke správci front, získá zprávu z fronty vstupů/požadavků, zkontroluje, zda je formát JSON správně naformátován, a pak vydá požadavek REST do blockchainu. Data vrácená technologií blockchain jsou analyzována mostem a umístěna do fronty odpovědí, jak je definováno v původní zprávě požadavku IBM MQ . Uživatelská aplikace se může připojit ke správci front, načíst zprávu odpovědi z fronty odpovědí a použít informace.



Obrázek 99. IBM MQ Bridge to blockchain

Musíte nakonfigurovat produkt IBM MQ Bridge to blockchain tak, aby se připojoval k serveru Hyperledger Composer REST, a nikoli přímo k základní vrstvě Hyperledger Fabric . Když je most spuštěn, aplikace systému zpráv požádá most o řízení rozhraní REST API produktu Hyperledger Composer na základě uživatelem definovaného modelu obchodní sítě, který následně řídí základní rutiny řetězového kódu, které mohou dotazovat nebo aktualizovat stav prostředku, a vrátí výsledky jako odezvu pomocí serveru Hyperledger Composer REST do aplikace systému zpráv.

Postup

Vytvořte fronty pro most úpravou a odesláním ukázkového JCL v souboru `thlqual.SCSQPROC(CSQ4BCBQ)`.

Pro výchozí pojmenované fronty, které se používají pro:

- Vstup zprávy do mostu: `SYSTEM.BLOCKCHAIN.INPUT.QUEUE`a `APPL1.BLOCKCHAIN.INPUT.QUEUE`
- Odpovědi od blockchainu: `APPL1.BLOCKCHAIN.REPLY.QUEUE`

Různé aplikace mohou používat stejnou vstupní frontu, ale můžete zadat více front odpovědí, jednu pro každou z vašich aplikací. Nemusíte používat definované fronty odpovědí. Chcete-li pro odpovědi použít dynamické fronty, musíte zvážit jejich konfiguraci zabezpečení.

Výsledky

Vytvořili jste fronty, které most vyžaduje pro zpracování zpráv z produktu IBM MQ a vaší blockchainové sítě.

Jak pokračovat dále

Pomocí informací pro správce front a pověření z blockchainové sítě vytvořte konfigurační soubor pro IBM MQ Bridge to blockchain.

Deprecated z/OS MQ Adv. VUE Vytvoření konfiguračního souboru pro IBM MQ Bridge to blockchain on z/OS

Zadáním parametrů správce front a sítě blockchain vytvořte konfigurační soubor pro připojení produktu IBM MQ Bridge to blockchain k sítím IBM MQ a IBM Blockchain .

Než začnete

Notes:

- Deprecated Produkt IBM MQ Bridge to blockchain je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-341). Blockchain konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.
- Removed V 9.3.2 Pro Continuous Deliveryse IBM MQ Bridge to blockchain odebere z produktu na adrese IBM MQ 9.3.2.
- LTS IBM zamýšlí odebrat schopnost z vydání Long Term Support v nadcházejících opravných sadách. Máte-li aplikace, které budou touto změnou ovlivněny, obraťte se na podporu IBM .
- Vytvořili jste a nakonfigurovali síť blockchainu Hyperledger Composer .
- Nainstalovali jste produkt IBM MQ Bridge to blockchain do svého prostředí z/OS .
- Spustili jste správce front IBM MQ Advanced for z/OS VUE .

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným pro vytvoření konfiguračního souboru IBM MQ Bridge to blockchain a úspěšné připojení k sítím IBM Blockchain a IBM MQ .

Most můžete použít pro připojení k sítím blockchainu, které jsou založeny na Hyperledger Composer. Chcete-li použít most, potřebujete informace o konfiguraci ze sítě blockchain. V každém kroku této úlohy najdete příklad podrobností konfigurace, které jsou založeny na dvou různě nakonfigurovaných sítích blockchain:

- Hyperledger Composer síť, která běží v Docker. Další informace viz Instalace Hyperledger Composera Generování rozhraní REST API.
- Hyperledger Composer síť, která běží v Kubernetes klastru v IBM Cloud. Další informace viz téma Vývoj v cloudovém sandboxu na platformě IBM Blockchain Platform.

Postup

1. Spusťte most ve svém prostředí z/OS UNIX System Services (z/OS UNIX) a vytvořte konfigurační soubor.

   Potřebujete parametry z informací o zabezpečení produktu Hyperledger Composer a ze správce front produktu IBM MQ Advanced for z/OS VUE .

   Spusťte skript mostu z adresáře `mqbc/bin` umístění v adresáři z/OS UNIX , kde je nainstalován produkt IBM MQ .

   ```
   ./runmqbcb -o config_file_name.cfg
   ```

   Jak ukazuje následující příklad, existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte klávesu `Enter` , abyste přijali existující hodnoty, stiskněte klávesu `Space` a poté `Enter` , abyste vymazali hodnoty, a zapište do hranatých závorek, pak stiskněte klávesu `Enter` , abyste přidali nové hodnoty. Seznamy hodnot (například rovnocenných hodnot) můžete oddělit čárkami nebo zadáním každé hodnoty na nový řádek. Seznam končí prázdným řádkem.

   Poznámka: Existující hodnoty nelze upravit. Můžete je zachovat, nahradit nebo vymazat.
2. Zadejte hodnoty pro připojení ke správci front IBM MQ Advanced for z/OS VUE .

Minimální hodnoty potřebné pro připojení jsou název správce front a názvy vstupních front mostu, které jste definovali. Pro připojení ke vzdáleným správcům front IBM MQ Advanced for z/OS VUE potřebujete také **MQ Channel** a **MQ Conname** (adresu hostitele a port, kde je správce front spuštěn).

Chcete-li použít TLS pro připojení k IBM MQ v kroku “5” na stránce 864, musíte použít rozhraní JNDI nebo CCDT a odpovídajícím způsobem zadat **MQ CCDT URL** nebo **JNDI implementation class** a **JNDI provider URL** .

Poznámka: Hodnoty **MQ CCDT** nebo **JNDI** mají přednost před konfiguračním souborem, kde se hodnoty překrývají.

```
Connection to Queue Manager
---------------------------
Queue Manager                       : [z/OS_ADV_VUE_qmgr_name]
Bridge Input Queue                  : [APPL1.BLOCKCHAIN.INPUT.QUEUE]
MQ Channel                          : []
MQ Conname                          : []
MQ CCDT URL                         : []
JNDI implementation class           : []
JNDI provider URL                   : []
MQ Userid                           : []
MQ Password                         : []
```

3. Zadejte pověření pro server Hyperledger Composer REST přidružený k síti blockchain (je-li nakonfigurována).

   V následujícím příkladu byl server Hyperledger Composer REST nakonfigurován s úložištěm pověření LDAP pomocí modulu **passport-ldapauth NodeJS** . Všimněte si, že můžete použít libovolný z modulů **passport-*** , které tímto způsobem poskytují základní pověření ve stylu uživatele a hesla. Další informace viz Povolení ověření pro server REST.

```
User Identification
-------------------------------
Userid                          : []admin
Password                        : []******
API path for Login              : auth/ldap
```

4. Zadejte adresu pro server Hyperledger Composer REST.

   Všimněte si, že v tomto atributu není potřeba žádný protokol, tj. `http` nebo `https`, a že číslo portu je povinné. To, zda se používá protokol HTTP nebo HTTPS , závisí na konfiguraci zabezpečení serveru REST. Pokud je serveru REST poskytnut certifikát a dvojice soukromých klíčů, použije se HTTPS . Používá se protokol HTTPS . Jinak se použije HTTP . Chcete-li získat informace o tom, jak zadat dvojici certifikátu a soukromého klíče, prohlédněte si krok “5” na stránce 864.

```
REST Server
---------------------------
Address for Composer REST server    : [composer-rest-server-ip-address:3000]
```

5. Zadejte hodnoty úložiště certifikátů pro připojení TLS.

   Most se chová jako klient produktu IBM MQ JMS , který se připojuje ke správci front, což znamená, že jej lze nakonfigurovat tak, aby používal zabezpečení TLS pro zabezpečené připojení stejným způsobem jako kterýkoli jiný klient produktu IBM MQ JMS . Konfigurace podrobností o připojení TLS je vystavena pouze po zadání informací o rozhraní JNDI nebo CCDT v kroku “2” na stránce 863.

   Úložiště certifikátů se používají pro produkt Hyperledger Composera pro vašeho správce front IBM MQ Advanced for z/OS VUE . Pokud jsou určena úložiště certifikátů, most se vždy pokusí připojit k serveru Hyperledger REST pomocí protokolu HTTPS. Protokol TLS však může být pro připojení systému IBM MQ zakázán, zatímco pro systém Hyperledger Composer stále používá protokol TLS s použitím následující volby.

```
Certificate stores for TLS connections
--------------------------------------
Personal keystore                   : []
Keystore password                   : []
Trusted store for signer certs      : []
Trusted store password              : []
```

```
Use TLS for MQ connection            : [N]
Timeout for Blockchain operations    : [12]
```

Další informace viz Zabezpečení serveru REST pomocí HTTPS a TLS.

6. Volitelné: Zadejte umístění souboru protokolu pro IBM MQ Bridge to blockchain.

   Název a umístění souboru protokolu můžete zadat v konfiguračním souboru nebo na příkazovém řádku.

```
Behavior of bridge program
--------------------------
Runtime logfile for copy of stdout/stderr : [/var/mqm/errors/runmqbcb.log]
Done.
```

Výsledky

Vytvořili jste konfigurační soubor, který produkt IBM MQ Bridge to blockchain používá pro připojení k síti IBM Blockchain a ke správci front IBM MQ Advanced for z/OS VUE .

Jak pokračovat dále

Projděte kroky pro “Spuštění IBM MQ Bridge to blockchain na z/OS” na stránce 866

Deprecated z/OS MQ Adv. VUE IBM MQ konfigurace zabezpečení pro IBM MQ Bridge to blockchain on z/OS

Aspekty pro nastavení zabezpečení systému IBM MQ pomocí konzoly IBM MQ Bridge to blockchain.

Notes:

- Deprecated Produkt IBM MQ Bridge to blockchain je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-341). Blockchain konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.
- Removed V 9.3.2 Pro Continuous Deliveryse IBM MQ Bridge to blockchain odebere z produktu na adrese IBM MQ 9.3.2.

Následující příklady ukazují definice RACF , které lze použít k poskytnutí přístupu IBM MQ Bridge to blockchain k frontám, které potřebuje. Definice předpokládají, že most je spuštěn pod ID uživatele MQBCBUSR.

Kromě toho musí být produktu IBM MQ Bridge to blockchain udělen přístup pro připojení ke správci front, a to buď:

- přímo pomocí režimu vazeb; viz Profily zabezpečení připojení pro dávková připojení, nebo
- Použití režimu klienta prostřednictvím příkazu CHINIT; viz Požadavky MQI klienta .

Autorizace pro frontu požadavků IBM MQ Bridge to blockchain

Zadáním následujících příkazů RACF udělte ID uživatele MQBCBUSR pro příjem zpráv z výchozího systému SYSTEM.BLOCKCHAIN.INPUT.QUEUE :

```
RDEFINE MQQUEUE SYSTEM.BLOCKCHAIN.INPUT.QUEUE UACC(NONE)
PERMIT SYSTEM.BLOCKCHAIN.INPUT.QUEUE CLASS(MQQUEUE) ID(MQBCBUSR) ACCESS(UPDATE)
```

Autorizace pro frontu odpovědí IBM MQ Bridge to blockchain

Zadáním následujících příkazů RACF udělte ID uživatele MQBCBUSR pro odesílání zpráv do aplikace APPL1.BLOCKCHAIN.REPLY.QUEUE. Tento název fronty je uveden v názvu fronty odpovědi na zprávu požadavku:

```
RDEFINE MQQUEUE APPL1.BLOCKCHAIN.REPLY.QUEUE UACC(NONE)
PERMIT APPL1.BLOCKCHAIN.REPLY.QUEUE CLASS(MQQUEUE) ID(MQBCBUSR) ACCESS(UPDATE)
PERMIT CONTEXT.APPL1.BLOCKCHAIN.REPLY.QUEUE CLASS(MQADMIN) ID(MQBCBUSR) ACCESS(UPDATE)
```

Související pojmy

Profily pro zabezpečení fronty

Související úlohy

“Spuštění ukázky klienta IBM MQ Bridge to blockchain v systému z/OS” na stránce 858

Pomocí ukázky klienta JMS , která je součástí produktu IBM MQ Bridge to blockchain, můžete vložit zprávu do vstupní fronty, kterou most blockchain kontroluje, a zobrazit přijatou odpověď. Tato ukázka je založena na použití produktu IBM MQ Bridge to blockchain , který je integrován s příkladem sítě Hyperledger Composer Trader.

Související odkazy

Rychlý odkaz na přístup k zabezpečení prostředků rozhraní API

Deprecated z/OS MQ Adv. VUE Spuštění IBM MQ Bridge to blockchain na z/OS

Spusťte IBM MQ Bridge to blockchain pro připojení k IBM Blockchain a IBM MQ. Po připojení je most připraven zpracovat zprávy požadavků, odeslat je do sítě blockchainu Hyperledger Composer a přijmout a zpracovat odpovědi.

Než začnete

Notes:

- Deprecated Produkt IBM MQ Bridge to blockchain je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-341). Blockchain konektivitu lze dosáhnout pomocí funkcí IBM App Connect nebo App Connect , které jsou k dispozici s produktem IBM Cloud Pak for Integration.
- Removed V 9.3.2 Pro Continuous Deliveryse IBM MQ Bridge to blockchain odebere z produktu na adrese IBM MQ 9.3.2.

Informace o této úloze

Ke spuštění úlohy IBM MQ Bridge to blockchainpoužijte konfigurační soubor, který jste vytvořili v předchozí úloze.

Postup

1. Spusťte správce front IBM MQ Advanced for z/OS VUE , kterého chcete použít s mostem.
2. Spuštěním rozhraní IBM MQ Bridge to blockchain se připojte k síti blockchainu a ke správci front produktu IBM MQ Advanced for z/OS VUE .

   Proveďte jednu z následujících akcí:

   a) Spusťte most přímo v adresáři z/OS UNIX System Services (z/OS UNIX) z adresáře `mqbc/bin` v umístění z/OS UNIX , kde je nainstalován produkt IBM MQ .

   ```
   ./runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/logFile.log
   ```

   , nebo

   b) b. Spusťte most ve svém systému z/OS s použitím ukázkového kódu JCL, který je uveden v souboru `thlqual.SCSQPROC(CSQ4BCB)`.

   Musíte provést řadu aktualizací JCL, které jsou specifické pro vaše prostředí:

   - Nahraďte ++THLQUAL++ kvalifikátorem vysoké úrovně datových sad cílové knihovny IBM MQ .
   - Nahraďte ++LANGLETTER++ písmenem pro jazyk, ve kterém chcete zobrazovat zprávy.

- Nahraďte proměnnou ++PATHPREFIX++ instalační cestou komponenty z/OS UNIX .
- Nahraďte proměnnou ++CONFIGFILE++ cestou ke konfiguračnímu souboru vytvořenému pomocí příkazu `runmqbc -o <file>` z adresáře z/OS UNIX.
- Nahraďte ++JAVAHOME++ umístěním 64bitového prostředí Java Virtual Machine (JVM) spuštěného v Java 8 nebo novějším.

Je-li most připojen, je vrácen výstup podobný následujícímu:

```
2018-05-17 14:28:16.866 BST IBM MQ Bridge to Blockchain
5724-H72 (C) Copyright IBM Corp. 2017, 2024.

2018-05-17 14:28:19.331 BST Ready to process input messages.
```

3. Volitelné: Odstraňte problémy s připojením ke správci front IBM MQ Advanced for z/OS VUE a k síti blockchain, pokud zprávy vrácené po spuštění mostu indikují, že připojení nebylo úspěšné.
   a) Zadejte příkaz v režimu ladění s volbou ladění 1.

   ```
   ./runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/
   logFile.log -d 1
   ```

   Most prochází nastaveným připojením a zobrazuje zprávy o zpracování v režimu "terse".
   b) Zadejte příkaz v režimu ladění s volbou ladění 2.

   ```
   ./runmqbcb -f /config_file_location/config_file_name.cfg -r /log_file_location/
   logFile.log -d 2
   ```

   Most prochází nastaveným připojením a zobrazuje zprávy zpracování v režimu s komentářem. Úplný výstup je zapsán do vašeho souboru protokolu.

Všimněte si, že volitelně můžete také určit volby režimu ladění v rámci JCL změnou `'-d 0'` na `'-d 1'` nebo `'-d 2'`.

Výsledky

Spustili jste produkt IBM MQ Bridge to blockchain a připojili jste se ke správci front a síti blockchain.

Jak pokračovat dále

- Chcete-li formátovat a odeslat dotaz nebo zprávu o aktualizaci do sítě blockchain, postupujte podle pokynů v části “Spuštění ukázky klienta IBM MQ Bridge to blockchain v systému z/OS” na stránce 858 .
- Použijte proměnnou *MQBCB_EXTRA_JAVA_OPTIONS* k předání vlastností prostředí JVM, například k povolení trasování IBM MQ . Další informace viz Trasování IBM MQ Bridge to blockchain.

Deprecated z/OS Formáty zpráv pro IBM MQ Bridge to blockchain před IBM MQ 9.2.0 na z/OS

Informace o formátování zpráv, které jsou odesílány a přijímány produktem IBM MQ Bridge to blockchain.

Upozornění: Existující formát pro formáty zpráv je zastaralý. V systému IBM MQ 9.2.0, pokud máte síť Hyperledger Fabric , použijte formát zpráv popsaných v části “Formáty zpráv pro IBM MQ Bridge to blockchain z IBM MQ 9.2.0” na stránce 853.

Aplikace požaduje, aby produkt IBM MQ Bridge to blockchain řídil rozhraní REST API definované produktem Hyperledger Composer , aby jednal s informacemi, které jsou zadrženy na blockchainu. Aplikace to provede umístěním zprávy požadavku do fronty požadavků mostu. Výsledky požadavku REST jsou zformátovány mostem do zprávy odpovědi. Most používá informace obsažené v polích **ReplyToQ** a **ReplyToQMgr** z deskriptoru MQMD zprávy požadavku jako místo určení pro zprávu odpovědi.

Zprávy požadavku a odpovědi jsou textové zprávy (MQSTR) ve formátu JSON.

Formát zprávy požadavku

Zprávy požadavků obsahují tři atributy:

metoda
Příkaz REST použitý k volání rozhraní REST API produktu Hyperledger Composer , jako např. POST, DELETE nebo GET

cesta
Cesta k rozhraní Hyperledger Composer REST API. Toto se přidá na základní server URL. Cesta by měla začínat na "`api/`".

tělo
Obsah specifický pro danou metodu. Toto je často struktura JSON.

Následující příklad používá metodu POST pro cestu `api/Traderk` vytvoření nového objektu Trader. Tělo specifikuje třídu Traders, jak je definována v modelu Hyperledger Composer uživatele, a také specifikuje další hodnoty potřebné k vytvoření nového objektu Trader v rámci blockchainové sítě.

```
{ "method": "POST",
  "path": "api/Trader",
  "body": {
    "$class" : "org.example.trading",
    "tradeId" : "Trader2",
    "firstName": "Jane",
    "lastName" : "Doe"
```

Formát zprávy odpovědi

Zprávy odpovědí mají své ID korelace nastaveno na ID zprávy příchozí zprávy. Všechny vlastnosti definované uživatelem se zkopírují ze zprávy požadavku do zprávy odpovědi. ID uživatele v odpovědi je nastaveno na ID uživatele původce.

`statusCode` je stavový kód HTTP . Pokud je chyba z IBM MQ nebo mostu, použije se odpovídající hodnota **`statusCode`** .

`statusType` je řetězec, buď *ÚSPĚCH* , nebo *SELHÁNÍ*.

V případě úspěšných požadavků obsahuje prvek "**`data`**" ve zprávě odpovědi odezvu z vyvolaného rozhraní Hyperledger Composer REST API.

Příklad úspěšného zpracování:

```
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "data": [
      {
         "$class": "org.example.trading",
         "firstName": "John",
         "lastName": "Doe",
         "tradeId": "Trader1"
      },
      {
         "$class": "org.example.trading",
         "firstName": "Jane",
         "lastName": "Doe",
         "tradeId": "Trader2"
      }
   ]
}
```

Všechny chybové odpovědi mají stejná pole, bez ohledu na to, zda jsou generovány samotným mostem, z volání na server Hyperledger Composer REST, blockchain nebo z vyvolání řetězového kódu. Příklad:

- Chybná vstupní zpráva JSON

```
 {
```

```
   "statusCode": 400,
   "statusType": "FAILURE",
   "message": "[AMQBC021E] Error: Cannot parse input message or there are
    missing fields in the message. Missing fields appear to be: "method"."
}
```

- Požadavek, který se nepodařilo zpracovat serverem Hyperledger Composer REST

```
{
   "statusCode": 500,
   "statusType": "FAILURE",
   "message": "Error trying to invoke business network. Error: No valid responses
    from any peers.\nResponse from attempted peer comms was an error: Error: chaincode
    error (status: 500, message: Error: Failed to add object with ID 'Trader1'
    as the object already exists)"
}
```

Aplikace mohou určit, zda byl požadavek úspěšný nebo selhal, buď pohledem na řetězec **statusType** , nebo z existence datového pole. Pokud dojde k chybě při zpracování vstupní zprávy a most ji neodešle do blockchainu, hodnota vrácená z mostu je hodnota MQRC, obvykle **MQRC_FORMAT_ERROR**.

Deprecated z/OS Spuštění ukázky klienta IBM MQ Bridge to blockchain v systému z/OS

Pomocí ukázky klienta JMS , která je součástí produktu IBM MQ Bridge to blockchain, můžete vložit zprávu do vstupní fronty, kterou most blockchain kontroluje, a zobrazit přijatou odpověď. Tato ukázka je založena na použití produktu IBM MQ Bridge to blockchain , který je integrován s příkladem sítě Hyperledger Composer Trader.

Než začnete

Další informace viz /trade_network

Produkt IBM MQ Bridge to blockchain je spuštěn a je připojen ke správci front IBM MQ Advanced nebo IBM MQ Advanced for z/OS VUE a k síti blockchain.

Informace o této úloze

Vyhledejte ukázkovou aplikaci JMS (`ComposerBCBSamp.java`) v adresáři `samp` v souboru IBM MQ Bridge to blockchain.

Například: `<MQ_INSTALL_ROOT>/mqbc/samp/ComposerBCBSamp.java`, kde `<MQ_INSTALL_ROOT>` je:

- Linux Adresář, kde je nainstalován produkt IBM MQ
- z/OS Adresář z/OS UNIX System Services , kde jsou nainstalovány komponenty z/OS UNIX produktu IBM MQ

.

Postup

1. Upravte ukázkový zdrojový soubor Java klienta.

   Postupujte podle pokynů v ukázce a nakonfigurujte jej tak, aby odpovídal vašemu prostředí IBM MQ a vaší blockchainové síti.

   Následující kód z ukázky definuje tři zprávy požadavku JSON, které se mají odeslat na most:

   a. Za prvé, odstranit existující '`commodity`'

   b. Za druhé, chcete-li vytvořit nové '`commodity`', '`owner`' a přidružené hodnoty,

c. Nakonec zobrazí nové informace o 'commodity' po předchozích dvou zprávách požadavku.

```
private static JSONObject[] createMessageBodies() {
    JSONObject[] msgs = new JSONObject[3]; // This method creates 3 messages
    JSONObject m, m2;
    String commodityName = "BC";

    // Clean out the commodity in case it's already there. If
    // it's not there, there will be an error returned from Composer.
    m = new JSONObject();
    m.put("method", "DELETE");
    m.put("path", "api/Commodity/" + commodityName);
    msgs[0] = m;

    // To add the item to the table, the
    // operation looks like this:
    //
    // { "method": "POST",
    //   "path": "api/Commodity",
    //   "body" : {
    //     "$class": "org.example.trading.Commodity",
    //     "tradingSymbol" : "BC",
    //     "description" : "BC",
    //     "mainExchange" : "HERE",
    //     "owner" : "Me",
    //     "quantity" : 100
    //   }
    // }
    // You can see this structure in the API Explorer
    m = new JSONObject();
    m.put("method", "POST");
    m.put("path", "api/Commodity");
    m2 = new JSONObject();
    m2.put("$class", " org.example.trading.Commodity");
    m2.put("tradingSymbol", commodityName);
    m2.put("description", "Blockchain Sample Description");
    m2.put("mainExchange", "My Exchange");
    m2.put("owner", "Me");
    m2.put("quantity", 100);
    m.put("body", m2);
    msgs[1] = m;

    // And list all items that have been created
    m = new JSONObject();
    m.put("method", "GET");
    m.put("path", "api/Commodity");
    msgs[2] = m;

    return msgs;
  }
```

2. Zkompilujte ukázku.

   Odkažte na třídy klienta IBM MQ a soubor JSON4J.jar , které jsou dodávány v adresáři mostu.

```
javac -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar
ComposerBCBClient.java
```

3. Spusťte kompilovanou třídu.

```
java -cp <MQ_INSTALL_ROOT>/java/lib/*:<MQ_INSTALL_ROOT>/mqbc/prereqs/JSON4J.jar:.
ComposerBCBClient
```

```
Starting Simple MQ Blockchain Bridge Client
Starting the connection.
Sent message:
  {"method":"DELETE"," path ":"api\/Commodity\/BC"}
Response text:
{
   "statusCode": 204,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": ""
}
```

```
SUCCESS
Sent message:
{"body":
{"$class":"org.example.trading.Commodity","owner":"Me","quantity":100,"description":"Blockcha
in Sample Description","mainExchange":"My
Exchange","tradingSymbol":"BC"},"operation":"POST","url":"Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": {
      "$class": "org.example.trading.Commodity",
      "description": "Blockchain Sample Description",
      "mainExchange": "My Exchange",
      "owner": "Me",
      "quantity": 100,
      "tradingSymbol": "BC"
   }
}
SUCCESS
Sent message:
  {"method":"GET","path":"api\/Commodity"}
Response text:
{
   "statusCode": 200,
   "statusType": "SUCCESS",
   "message": "OK",
   "data": [
      {
         "$class": "org.example.trading.Commodity",
         "description": "Blockchain Sample Description",
         "mainExchange": "My Exchange",
         "owner": "resource:org.example.trading.Trader#Me",
         "quantity": 100,
         "tradingSymbol": "BC"
      }
   ]
}
SUCCESS
```

Pole **message** obsahuje buď "OK" pro úspěšně zpracovanou zprávu, nebo v případě nezdařeného požadavku informace týkající se příčiny selhání.

Pokud klient obdrží chybu časového limitu při čekání na odezvu, zkontrolujte, zda je most spuštěn.

z/OS Konfigurace správců front v systému z/OS

Pomocí těchto pokynů můžete konfigurovat správce front v systému IBM MQ for z/OS.

Než začnete

Před konfigurací produktu IBM MQ for z/OSsi přečtěte:

- IBM MQ for z/OS koncepty
- Plánování prostředí IBM MQ na z/OS

Informace o této úloze

Po instalaci produktu IBM MQmusíte provést řadu úloh, než jej budete moci zpřístupnit uživatelům.

Procedura

- Informace o způsobu konfigurace správců front v systému IBM MQ for z/OSnaleznete v následujících dílčích tématech.

Související pojmy

z/OS Zdroje, ze kterých můžete zadat příkazy MQSC a PCF na systému IBM MQ for z/OS

Související úlohy

“Vytvoření správců front na platformě Multiplatforms” na stránce 7
Než budete moci používat zprávy a fronty, musíte vytvořit a spustit alespoň jednoho správce front a jeho přidružené objekty. Správce front spravuje přidružené prostředky, zejména fronty, které vlastní. Poskytuje služby řazení do front pro aplikace pro volání rozhraní MQI (Message Queueing Interface) a příkazy pro vytváření, úpravy, zobrazování a odstraňování objektů IBM MQ .

Zabezpečení

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

“Konfigurace připojení mezi klientem a serverem” na stránce 14
Chcete-li konfigurovat komunikační spojení mezi produktem IBM MQ MQI clients a servery, rozhodněte se o svém komunikačním protokolu, definujte připojení na obou koncích linky, spusťte modul listener a definujte kanály.

z/OS Správa serveruIBM MQ for z/OS

Naplánování

Související odkazy

z/OS Použití obslužných programů IBM MQ for z/OS

z/OS Příprava na přizpůsobení správců front v systému z/OS

Toto téma použijte při úpravě správců front s podrobnostmi o instalovatelných funkcích, funkcích v národním jazyce a informacích o testování a nastavení zabezpečení.

Příprava na přizpůsobení

Programový adresář uvádí obsah instalační pásky IBM MQ , informace o programu a servisní úrovni pro systém IBM MQa popisuje, jak nainstalovat produkt IBM MQ for z/OS pomocí SMP/E (System Modification Program Extended). Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Po instalaci produktu IBM MQmusíte provést řadu úloh, než jej budete moci zpřístupnit uživatelům. Popis těchto úloh naleznete v následujících sekcích:

- “nastaveníIBM MQ for z/OS” na stránce 876
- “Testování správce front v systému z/OS” na stránce 941
- Nastavení zabezpečení na systému z/OS

Pokud provádíte migraci z předchozí verze produktu IBM MQ for z/OS, nemusíte provádět většinu úloh přizpůsobení. Další informace o úlohách, které musíte provést, naleznete v tématu Údržba a migrace .

Instalovatelné funkce produktu IBM MQ for z/OS

Produkt IBM MQ for z/OS se skládá z následujících funkcí:

Základ
To je nutné; zahrnuje všechny hlavní funkce, včetně

- Administrace a obslužné programy
- Podpora aplikací CICS, IMSa dávkového typu pomocí rozhraní IBM MQ Application Programming Interface nebo C++
- Prostředek distribuovaného řazení do front (podporující komunikaci TCP/IP i APPC)

Funkce národního jazyka
Ty obsahují chybové zprávy a panely ve všech podporovaných národních jazycích. Ke každému jazyku je přidružen jazykový dopis. Jazyky a písmena jsou:

C
Zjednodušená čínština

E
U.S. Angličtina (malá i velká písmena)

F
Francouzština

K
Japonština

U
U.S. Angličtina (velká písmena)

Musíte nainstalovat volbu US English (smíšená velká a malá písmena). Můžete také nainstalovat jeden nebo více dalších jazyků. (Proces instalace pro jiné jazyky vyžaduje, aby byla nainstalována americká angličtina (smíšená velikost písmen), a to i v případě, že nebudete používat americkou angličtinu (smíšená velikost písmen).)

IBM MQ for z/OS UNIX System Services Components
Tato funkce je volitelná. Tuto funkci vyberte, chcete-li sestavit a spustit aplikace Java , které používají produkt Jakarta Messaging 3.0 nebo Java Message Service 2.0 pro připojení k produktu IBM MQ for z/OS.

Informace o instalaci produktu IBM MQ for z/OS UNIX System Services Componentsnaleznete v tématu IBM MQ for z/OS Soubory PDF adresáře programu .

IBM MQ for z/OS UNIX System Services Web Components
Tato funkce je volitelná.

Tuto funkci vyberte, chcete-li použít IBM MQ Consolenebo REST API.

Chcete-li nainstalovat tuto funkci, musíte nainstalovat funkci IBM MQ for z/OS UNIX System Services Components .

IBM MQ for z/OS Managed File Transfer
Tato funkce je volitelná a měla by být nainstalována pouze v případě, že máte nárok na IBM MQ Advanced for z/OS, IBM MQ for z/OS Value Unit Edition (VUE)nebo IBM MQ for z/OS Managed File Transfer.

Tuto funkci vyberte, chcete-li použít Managed File Transfer schopnosti produktu IBM MQ for z/OS.

Chcete-li nainstalovat tuto funkci, musíte nainstalovat funkci IBM MQ for z/OS UNIX System Services Components .

Knihovny, které existují po instalaci

Produkt IBM MQ je dodáván s řadou samostatných zaváděcích knihoven. Tabulka 53 na stránce 873 zobrazuje knihovny, které mohou existovat po instalaci produktu IBM MQ.

Tabulka 53. Knihovny IBM MQ , které existují po instalaci

Název	Popis
thlqual.SCSQANLC	Obsahuje zaváděcí moduly pro zjednodušenou čínskou verzi produktu IBM MQ.
thlqual.SCSQANLE	Obsahuje zaváděcí moduly pro U.S. Anglická (smíšená) verze produktu IBM MQ.
thlqual.SCSQANLF	Obsahuje zaváděcí moduly pro francouzskou verzi produktu IBM MQ.
thlqual.SCSQANLK	Obsahuje zaváděcí moduly pro japonskou verzi produktu IBM MQ.
thlqual.SCSQANLU	Obsahuje zaváděcí moduly pro U.S. Anglická (velká písmena) verze produktu IBM MQ.

Tabulka 53. Knihovny IBM MQ , které existují po instalaci (pokračování)	
Název	**Popis**
thlqual.SCSQASMS	Obsahuje zdroj pro ukázkové programy assembleru.
thlqual.SCSQAUTH	Hlavní úložiště pro všechny zaváděcí moduly produktu IBM MQ ; obsahuje také výchozí modul parametrů CSQZPARM. Tato knihovna musí mít autorizaci APF a musí být ve formátu PDS-E.
thlqual.SCSQCICS	Obsahuje další zaváděcí moduly, které musí být zahrnuty do zřetězení CICS DFHRPL. Tato knihovna musí mít autorizaci APF a musí být ve formátu PDS-E.
thlqual.SCSQCLST	Obsahuje CLISTy používané vzorovými programy.
thlqual.SCSQCOBC	Obsahuje zakladače COBOL, včetně zakladačů požadovaných pro ukázkové programy.
thlqual.SCSQCOBS	Obsahuje zdroj pro ukázkové programy v jazyce COBOL.
thlqual.SCSQCPPS	Obsahuje zdroj pro ukázkové programy C + +.
thlqual.SCSQC37S	Obsahuje zdroj pro ukázkové programy jazyka C.
thlqual.SCSQC370	Obsahuje záhlaví C, včetně záhlaví požadovaných pro ukázkové programy.
thlqual.SCSQDEFS	Obsahuje boční definice pro C++ a Db2 DBRM pro sdílené řazení do front.
thlqual.SCSQEXEC	Obsahuje spustitelné soubory REXX, které mají být zahrnuty do zřetězení SYSEXEC nebo SYSPROC, pokud používáte operace IBM MQ a ovládací panely.
thlqual.SCSQFCMD	Obsahuje šablony pro úlohy k vytvoření a spuštění úloh Managed File Transfer .
thlqual.SCSQHPPS	Obsahuje soubory záhlaví pro C + +.
thlqual.SCSQINST	Obsahuje JCL pro instalační úlohy.
thlqual.SCSQLINK	Předběžná kódová knihovna. Obsahuje zaváděcí moduly, které jsou zavedeny při IPL (system initial program load). Knihovna musí mít autorizaci APF.
thlqual.SCSQLOAD	Zaveďte knihovnu. Obsahuje zaváděcí moduly pro jiný kód než APF, uživatelské procedury, obslužné programy, ukázky, programy pro ověření instalace a stuby adaptéru. Knihovna nemusí mít autorizaci APF a nemusí být v seznamu odkazů. Tato knihovna musí být ve formátu PDS-E.
thlqual.SCSQMACS	Obsahuje makra asembleru včetně: ukázkových maker, maker produktu a maker systémových parametrů.
thlqual.SCSQMAPS	Obsahuje sady map CICS používané ukázkovými programy.
thlqual.SCSQMSGC	Obsahuje zprávy ISPF , které se mají zahrnout do zřetězení ISPMLIB, pokud používáte funkci zjednodušené čínštiny pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGE	Obsahuje zprávy ISPF , které se mají zahrnout do zřetězení ISPMLIB, pokud používáte U.S. Funkce anglického jazyka (smíšená velikost písmen) pro operace IBM MQ a ovládací panely.

Tabulka 53. Knihovny IBM MQ , které existují po instalaci (pokračování)

Název	Popis
thlqual.SCSQMSGF	Obsahuje zprávy ISPF , které se mají zahrnout do zřetězení ISPMLIB, pokud používáte funkci francouzského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGK	Obsahuje zprávy ISPF , které se mají zahrnout do zřetězení ISPMLIB, pokud používáte funkci japonského jazyka pro operace a ovládací panely IBM MQ .
thlqual.SCSQMSGU	Obsahuje zprávy ISPF , které se mají zahrnout do zřetězení ISPMLIB, pokud používáte U.S. Funkce anglického jazyka (velká písmena) pro operace IBM MQ a ovládací panely.
thlqual.SCSQMVR1	Obsahuje zaváděcí moduly pro distribuované řazení do front. Tato knihovna musí mít autorizaci APF a musí být ve formátu PDS-E.
thlqual.SCSQPLIC	Obsahuje soubory začlenění PL/I.
thlqual.SCSQPLIS	Obsahuje zdroj pro ukázkové programy PL/I.
thlqual.SCSQPNLA	Obsahuje panely IPCS pro formátovač výpisu paměti, které mají být zahrnuty do zřetězení ISPPLIB. Také obsahuje panely pro ukázkové programy IBM MQ .
thlqual.SCSQPNLC	Obsahuje panely ISPF , které se mají zahrnout do zřetězení ISPPLIB, pokud používáte funkci zjednodušené čínštiny pro operace a ovládací panely IBM MQ .
thlqual.SCSQPNLE	Obsahuje panely ISPF , které se mají zahrnout do zřetězení ISPPLIB, pokud používáte U.S. Funkce anglického jazyka (smíšená velikost písmen) pro operace IBM MQ a ovládací panely.
thlqual.SCSQPNLF	Obsahuje panely ISPF , které se mají zahrnout do zřetězení ISPPLIB, pokud používáte funkci francouzského jazyka pro operace a ovládací panely IBM MQ .
thlqual.SCSQPNLK	Obsahuje panely ISPF , které se mají zahrnout do zřetězení ISPPLIB, pokud používáte funkci japonského jazyka pro operace a ovládací panely IBM MQ .
thlqual.SCSQPNLU	Obsahuje panely ISPF , které se mají zahrnout do zřetězení ISPPLIB, pokud používáte U.S. Funkce anglického jazyka (velká písmena) pro operace IBM MQ a ovládací panely.
thlqual.SCSQPROC	Obsahuje ukázkové datové sady JCL a výchozí datové sady inicializace systému.
thlqual.SCSQSNLC	Obsahuje zaváděcí moduly pro zjednodušenou čínskou verzi modulů IBM MQ , které jsou vyžadovány pro speciální účelovou funkci (například raný kód).
thlqual.SCSQSNLE	Obsahuje zaváděcí moduly pro U.S. Anglická (smíšená) verze modulů IBM MQ , které jsou vyžadovány pro funkci pro speciální účel (například počáteční kód).
thlqual.SCSQSNLF	Obsahuje zaváděcí moduly pro francouzské verze modulů IBM MQ , které jsou nezbytné pro speciální funkci (například raný kód).
thlqual.SCSQSNLK	Obsahuje zaváděcí moduly pro japonské verze modulů IBM MQ , které jsou vyžadovány pro funkci speciálního určení (například raný kód).

Tabulka 53. Knihovny IBM MQ , které existují po instalaci (pokračování)	
Název	**Popis**
thlqual.SCSQSNLU	Obsahuje zaváděcí moduly pro U.S. Anglická (velká písmena) verze modulů IBM MQ , které jsou vyžadovány pro funkci speciálního určení (například počáteční kód).
thlqual.SCSQTBLC	Obsahuje tabulky ISPF , které se mají zahrnout do zřetězení ISPTLIB, pokud používáte funkci zjednodušená čínština pro operace a ovládací panely IBM MQ .
thlqual.SCSQTBLE	Obsahuje tabulky ISPF , které se mají zahrnout do zřetězení ISPTLIB, pokud používáte U.S. Funkce anglického jazyka (smíšená velikost písmen) pro operace IBM MQ a ovládací panely.
thlqual.SCSQTBLF	Obsahuje tabulky ISPF , které mají být zahrnuty do zřetězení ISPTLIB, pokud používáte funkci francouzského jazyka pro operace a ovládací panely IBM MQ .
thlqual.SCSQTBLK	Obsahuje tabulky ISPF , které se mají zahrnout do zřetězení ISPTLIB, pokud používáte funkci japonského jazyka pro operace a ovládací panely IBM MQ .
thlqual.SCSQTBLU	Obsahuje tabulky ISPF , které se mají zahrnout do zřetězení ISPTLIB, pokud používáte U.S. Funkce anglického jazyka (velká písmena) pro operace IBM MQ a ovládací panely.

Poznámka: Neupravujte ani neupravujte žádnou z těchto knihoven. Chcete-li provést změny, zkopírujte knihovny a proveďte změny v kopiích.

Související pojmy

IBM MQ for z/OS koncepce

“Použití IBM MQ s IMS” na stránce 980
Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

“Použití IBM MQ s CICS” na stránce 988
Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér IBM MQ CICS a volitelně komponenty produktu IBM MQ CICS bridge .

“Použití uživatelských procedur OTMA v adresáři IMS” na stránce 991
Toto téma použijte, chcete-li použít uživatelské procedury IMS Open Transaction Manager Access s produktem IBM MQ for z/OS.

Související úlohy

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 950
Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

Správa serveruIBM MQ for z/OS

Související odkazy

“Upgrade a použití služby v prostředí Language Environment nebo z/OS Callable Services” na stránce 988
Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a podle vaší verze SMP/E.

z/OS nastaveníIBM MQ for z/OS

Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

Nejlepším způsobem konfigurace správce front je provést následující kroky v uvedeném pořadí:

1. Konfigurujte základního správce front.
2. Konfigurujte inicializátor kanálu, který provádí správce front pro komunikaci se správci front, a komunikaci se vzdálenou klientskou aplikací.
3. Chcete-li šifrovat nebo chránit zprávy, nakonfigurujte Advanced Message Security for z/OS.
4. Chcete-li použít produkt IBM MQ k přenosu souborů, nakonfigurujte produkt Managed File Transfer for z/OS.
5. Chcete-li použít administraci nebo systém zpráv REST APInebo IBM MQ Console ke správě IBM MQ z webového prohlížeče, nakonfigurujte server mqweb.

Toto téma vás provede různými fázemi nastavení produktu IBM MQ po úspěšné instalaci. Proces instalace je popsán v adresáři Program Directory. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Ukázky jsou dodávány s produktem IBM MQ , který vám pomůže s přizpůsobením. Členové ukázkové datové sady mají názvy začínající čtyřmi znaky CSQ4 a jsou v knihovně thlqual.SCSQPROC.

Před provedením úloh přizpůsobení popsaných v tomto tématu existuje řada voleb konfigurace, které musíte zvážit, protože ovlivňují požadavky na výkon a prostředky produktu IBM MQ for z/OS. Musíte se například rozhodnout, které knihovny globalizace chcete použít.

Chcete-li automatizovat některé kroky přizpůsobení, viz “Použití produktu IBM z/OSMF k automatizaci IBM MQ” na stránce 995.

Volby konfigurace

Další informace o těchto volbách viz Plánování v z/OS.

Popis každé úlohy v této sekci označuje, zda:

- Úloha je součástí procesu nastavení IBM MQ. To znamená, že úlohu provedete jednou, když upravíte soubor IBM MQ na systému z/OS . (V paralelním prostředí sysplex musíte provést úlohu pro každý systém z/OS v prostředí sysplex a zajistit, aby byl každý systém z/OS nastaven stejně.)
- Úloha je součástí přidání správce front. To znamená, že úlohu provedete jednou pro každého správce front při přidávání tohoto správce front.

Žádná z úloh nevyžaduje, abyste provedli IPL systému z/OS , pokud použijete příkazy ke změně různých parametrů systému z/OS a provedete “Aktualizujte SYS1.PARMLIB” na stránce 891 podle návrhu.

Chcete-li zjednodušit operace a pomoci při určování problémů, ujistěte se, že všechny systémy z/OS v prostředí sysplex jsou nastaveny stejně, aby bylo možné rychle vytvořit správce front v libovolném systému v případě nouze.

Chcete-li usnadnit údržbu, zvažte definování aliasů tak, aby odkazovaly na vaše knihovny IBM MQ . Další informace naleznete v tématu Použití aliasu k odkazování na IBM MQ knihovnu.

Související pojmy

IBM MQ for z/OS koncepce

“Použití IBM MQ s IMS” na stránce 980
Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

“Použití IBM MQ s CICS” na stránce 988
Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér IBM MQ CICS a volitelně komponenty produktu IBM MQ CICS bridge .

“Použití uživatelských procedur OTMA v adresáři IMS” na stránce 991
Toto téma použijte, chcete-li použít uživatelské procedury IMS Open Transaction Manager Access s produktem IBM MQ for z/OS.

Související úlohy

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 950

Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

Správa serveruIBM MQ for z/OS

Související odkazy

“Upgrade a použití služby v prostředí Language Environment nebo z/OS Callable Services” na stránce 988

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a podle vaší verze SMP/E.

z/OS Konfigurace systému z/OS pro IBM MQ

Tato témata použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

z/OS *Identifikace parametrů systému z/OS*

Některé z úloh zahrnují aktualizaci systémových parametrů z/OS . Musíte vědět, které byly uvedeny při provádění IPL systému.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*

SYS1.PARMLIB(IEASYSpp) obsahuje seznam parametrů, které ukazují na ostatní členy SYS1.PARMLIB (kde pp představuje seznam systémových parametrů z/OS , který byl použit k provedení IPL systému).

Položky, které potřebujete najít, jsou:

Pro “Autorizace APF pro zaváděcí knihovny IBM MQ” na stránce 878:
PROG=xx nebo APF=aa ukazují na autorizovaný seznam knihoven APF (Authorized Program Facility) (člen PROGxx nebo IEFAPFaa)

Pro “Aktualizovat seznam odkazů z/OS a LPA” na stránce 879:
LNK=kk ukazuje na seznam odkazů (člen LNKLSTkk) LPA=mm ukazuje na seznam LPA (člen LPALSTmm)

Pro “Aktualizovat tabulku vlastností programu z/OS” na stránce 883:
SCH=xx ukazuje na tabulku vlastností programu (PPT) (člen SCHEDxx)

Pro “Definujte subsystém IBM MQ pro z/OS .” na stránce 884:
SSN=ss ukazuje na definovaný seznam subsystémů (člen IEFSSNss)

z/OS *Autorizace APF pro zaváděcí knihovny IBM MQ*

APF-autorizujte různé knihovny. Některé zaváděcí moduly již mohou být autorizovány.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že nastavení pro IBM MQ jsou identická na každém systému z/OS v prostředí sysplex.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*
- *Použití knihovny s odložením stranou (LLA):*
  - *Některé IBM MQ použití může způsobit vysoký vstup/výstup (IO) pro načtení modulů z knihoven. Tento I/O lze snížit pomocí zařízení LLA operačního systému.*
  - *K tomuto vysokému vstupu/výstupu může dojít během:*
    - *Aplikace s vysokou rychlostí MQCONN/MQDISC, například v uložené proceduře WLM.*
    - *Načítání uživatelských procedur kanálu. Máte-li kanály, které se spouštějí a zastavují často, a používáte-li uživatelské procedury kanálu.*
  - *Člen CSVLLAxx v SYS1.PARMLIB uvádí nastavení LLA. Zahrnutí názvu knihovny do příkazu LIBRARIES znamená, že kopie programu bude vždy převzata z VLF (Virtual Lookaside Facility), a proto nebude obvykle vyžadovat vstup/výstup, když je silně využíván.*

Zahrnutí do příkazu FREEZE znamená, že neexistuje žádný vstup/výstup pro získání příslušných adresářů zřetězení příkazů DD (může to být často více vstupů/výstupů, než je samotné načtení programu).

Použít příkaz operačního systému " F LLA, REFRESH " po všech změnách v některé z těchto knihoven.

IBM MQ zaváděcí knihovny thlqual.SCSQAUTH a thlqual.SCSQLINK musí mít autorizaci APF. Musíte také autorizovat APF knihovny pro funkci národního jazyka (thlqual.SCSQANLx a thlqual.SCSQSNLx) a pro funkci distribuovaného řazení do front (thlqual.SCSQMVR1).

Všechny zaváděcí moduly v LPA jsou však automaticky autorizovány APF. Takže jsou všichni členové seznamu odkazů, pokud je SYS1.PARMLIB člen IEASYSpp obsahuje příkaz:

```
LNKAUTH=LNKLST
```

LNKAUTH=LNKLST je předvolba, pokud není uvedena hodnota LNKAUTH.

V závislosti na tom, co se rozhodnete vložit do LPA nebo seznamu odkazů (viz “Aktualizovat seznam odkazů z/OS a LPA” na stránce 879), možná nebudete muset umístit knihovny do seznamu odkazů APF.

Poznámka: Musíte autorizovat APF všechny knihovny, které zahrnete do knihovny IBM MQ STEPLIB. Pokud do knihovny STEPLIB vložíte knihovnu, která nemá autorizaci APF, celá zřetězení knihoven ztratí autorizaci APF.

Seznamy APF jsou v SYS1.PARMLIB člen PROGxx nebo IEAAPFaa. Seznamy obsahují názvy autorizovaných knihoven z/OS APF. Pořadí položek v seznamech není významné. Informace o seznamech APF viz Seznam knihoven s oprávněním APF .

Další informace o vyladění systému viz SupportPac MP16

Používáte-li členy PROGxx s dynamickým formátem, musíte zadat pouze z/OS příkaz SETPROG APF,ADD,DSNAME=hlq.SCSQ *XXXX*,VOLUME= *YYYYYY* , aby se změny projevily: Kde *XXXX* se liší podle názvu knihovny a kde *YYYYY* je svazek. Jinak, pokud používáte statický formát nebo členy IEAAPFaa, musíte provést IPL ve vašem systému.

Všimněte si, že musíte použít skutečný název knihovny v seznamu APF. Pokud se pokusíte použít alias datové sady knihovny, autorizace se nezdaří.

Související pojmy

“Aktualizovat seznam odkazů z/OS a LPA” na stránce 879
Aktualizujte knihovny LPA pomocí nové verze knihoven raného kódu. Další kód může jít v seznamu odkazů nebo LPA.

“Příprava na přizpůsobení správců front v systému z/OS” na stránce 872
Toto téma použijte při úpravě správců front s podrobnostmi o instalovatelných funkcích, funkcích v národním jazyce a informacích o testování a nastavení zabezpečení.

z/OS *Aktualizovat seznam odkazů z/OS a LPA*

Aktualizujte knihovny LPA pomocí nové verze knihoven raného kódu. Další kód může jít v seznamu odkazů nebo LPA.

- Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.
- Používáte-li skupiny sdílení front, měli byste aktualizovat počáteční kód v každém správci front v rámci skupiny sdílení front na úroveň IBM MQ 9.3.0 před migrací kteréhokoli ze správců front do adresáře IBM MQ 9.3.0.

  Nainstalujte nejnovější počáteční kód na každou oblast LPAR a poté aktualizujte správce front jeden po druhém v určitém okamžiku před migrací. Nemusíte migrovat všechny správce front současně.
- Možná budete muset provést tuto úlohu při migraci z předchozí verze. Další podrobnosti naleznete v adresáři Program Directory. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Poznámka: Datová sada pro LPA je specifická pro verzi. Používáte-li v systému existující LPA, obraťte se na administrátora systému a rozhodněte se, který LPA má použít.

Předčasné kódy

Některé IBM MQ zaváděcí moduly musí být přidány do MVS pro IBM MQ , aby fungovaly jako subsystém. Tyto moduly jsou označovány jako dřívější kód a lze je spustit i v případě, že správce front není aktivní. Je-li například v konzole zadán příkaz operátora s předponou příkazu IBM MQ , získá tento předběžný kód řízení a zkontroluje, zda potřebuje spustit správce front nebo předat požadavek spuštěnému správci front. Tento kód je načten do oblasti Link Pack Area (LPA). Existuje jedna sada modulů Early, které se používají pro všechny správce front, a ty musí být na nejvyšší úrovni IBM MQ. Dřívější kód z vyšší verze produktu IBM MQ bude pracovat se správcem front s nižší verzí produktu IBM MQ, nikoli však s opačnou verzí.

Počáteční kód se skládá z následujících zaváděcích modulů:

- CSQ3INI a CSQ3EPX v knihovně thqual.SCSQLINK
- CSQ3ECMX v knihovně thqual.SCSQSNL *x*, kde *x* je vaše jazykové písmeno:
  - thlqual.SCSQSNLE, pro anglickou smíšenou velikost písmen
  - thlqual.SCSQSNLU, pro americkou angličtinu velká písmena
  - thlqual.SCSQSNLK, pro japonštinu
  - thlqual.SCSQSNLF, pro francouzštinu
  - thlqual.SCSQSNLC, pro čínštinu

Produkt IBM MQ zahrnuje úpravu uživatele, která přesune obsah knihovny thqual.SCSQSNL *i* do thqual.SCSQLINK a informuje SMP/E. Tato uživatelská úprava se nazývá CSQ8UERL a je popsána v adresáři *Program Directory for IBM MQ for z/OS* pro Long Term Support nebo Continuous Delivery. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Pokud jste aktualizovali počáteční kód v knihovnách LPA, je k dispozici od příštího IPL systému z/OS (s volbou CLPA) pro všechny subsystémy správce front přidané během IPL z definic ve členech IEFSSNss v systému SYS1.PARMLIB.

Můžete jej zpřístupnit okamžitě bez IPL pro jakýkoli nový subsystém správce front přidaný později (jak je popsáno v tématu “Definujte subsystém IBM MQ pro z/OS .” na stránce 884). doplněním k LPA takto:

- Pokud jste nepoužili CSQ8UERL, zadejte tyto příkazy z/OS :

```
SETPROG LPA,ADD,MODNAME=(CSQ3INI,CSQ3EPX),DSNAME=thqual.SCSQLINK
SETPROG LPA,ADD,MODNAME=(CSQ3ECMX),DSNAME=thqual.SCSQSNL x
```

- Pokud jste použili CSQ8UERL, můžete načíst raný kód do LPA pomocí následujícího příkazu z/OS :

```
SETPROG LPA,ADD,MASK=*,DSNAME=thqual.SCSQLINK
```

- Používáte-li produkt Advanced Message Security , musíte také zadat následující příkaz z/OS , který zahrne další modul do LPA:

```
SETPROG LPA,ADD,MODNAME=(CSQ0DRTM),DSNAME=thqual.SCSQLINK
```

Pokud jste provedli údržbu nebo máte v úmyslu restartovat správce front s novější verzí nebo vydáním produktu IBM MQ, lze počáteční kód zpřístupnit existujícím správcům front pomocí následujících kroků. Správci front, kteří neprovádějí tyto kroky, nadále používají verzi raného kódu, kterou již používají. Tyto kroky není nutné provádět pro všechny správce front v oblasti LPAR, pokud se konkrétně nepokoušíte použít údržbu pro všechny z nich nebo je všechny aktualizovat na novější verzi nebo vydání produktu IBM MQ.

1. Přidejte jej do LPA pomocí příkazů z/OS SETPROG, jak bylo popsáno výše v tomto tématu.
2. Zastavte správce front pomocí příkazu IBM MQ STOP QMGR.

3. Ujistěte se, že qmgr.REFRESH.QMGR je nastaven. Viz Příkazy MQSC, profily a jejich úrovně přístupu.
4. Aktualizujte počáteční kód pro správce front pomocí příkazu IBM MQ REFRESH QMGR TYPE (EARLY).
5. Restartujte správce front pomocí příkazu IBM MQ START QMGR.

Příkazy IBM MQ STOP QMGR, REFRESH QMGR a START QMGR jsou popsány v části Příkazy MQSC.

Jiný kód

Všechny zaváděcí moduly dodávané s produktem IBM MQ v následujících knihovnách jsou reentrant a lze je umístit do LPA:

- SCSQAUTH
- SCSQANL *x*, kde *x* je vaše jazykové písmeno.
- SCSQMVR1

Důležité: Pokud však umístíte knihovny do LPA, kdykoli použijete údržbu, musíte ručně zkopírovat všechny změněné moduly do LPA. Proto je vhodnější umístit zaváděcí knihovny IBM MQ do seznamu odkazů, který lze aktualizovat po údržbě zadáním příkazu z/OS MODIFY LLA REFRESH.

Další informace viz Úprava obsahu datových sad LNKLST a Bezpečné a správné použití dynamického zařízení LNKLST.

To se doporučuje zejména pro SCSQAUTH, abyste jej nemuseli zahrnout do několika STEPLIB. Do LPA nebo seznamu odkazů by měla být umístěna pouze jedna jazyková knihovna SCSQANL *x* . Knihovny seznamu odkazů jsou uvedeny ve členu LNKLSTkk SYS1.PARMLIB.

Zařízení distribuovaných front a produkt CICS bridge (nikoli však samotný správce front) potřebují přístup k běhové knihovně SCEERUN jazykového prostředí (LE). Pokud používáte některé z těchto zařízení, musíte zahrnout SCEERUN do seznamu odkazů.

V 9.3.2 Některé moduly jsou načteny při spuštění správce front do ECSA. V omezených prostředích ECSA je možné tyto moduly umístit do LPA. Další informace viz “Umístění globálních modulů IBM MQ do LPA” na stránce 881.

Důležité: LTS Chcete-li použít toto zařízení v produktu IBM MQ 9.3 , musíte použít opravu APAR PH52358.

Související pojmy

“Aktualizovat tabulku vlastností programu z/OS” na stránce 883
Pro správce front IBM MQ jsou zapotřebí některé další položky PPT.

z/OS V 9.3.2 *Umístění globálních modulů IBM MQ do LPA*

Při spuštění správce front IBM MQ for z/OS načte některé své zaváděcí moduly (globální moduly) do rozšířené společné oblasti služeb (ECSA). Při vypnutí správce front je ECSA uvolněno.

Existuje 19 globálních modulů, které v systému IBM MQ 9.3spotřebovávají přibližně 1.2 MB ECSA pro každého spuštěného správce front.

Poznámka: Ačkoli je CSQ7GPLM globální modul, neměl by být přidán do LPA.

V prostředích, která spouštějí více správců front pro každou oblast LPAR a vyžadují snížení spotřeby ECSA kvůli ECSA nebo vysokým soukromým omezením, je možné umístit globální moduly do LPA. Umístění globálních modulů produktu IBM MQ do LPA je ruční proces, který vyžaduje péči, takže tento postup byste měli provést pouze v případě, že existuje významná potřeba řešit ECSA nebo vysoká soukromá omezení.

Důležité: LTS Chcete-li použít toto zařízení v produktu IBM MQ 9.3 , musíte použít opravu APAR PH52358.

Pokud správce front nemůže najít globální modul ve své knihovně STEPLIB a zjistí, že se modul nachází v LPA, použije kopii LPA přímo namísto načtení kopie modulu do ECSA. Případně, pokud je kód správců

front obvykle načten ze seznamu odkazů, pak jsou všechny globální moduly v LPA načteny přednostně před jakýmikoli globálními moduly v seznamu odkazů.

z/OS Funkce společného sledování úložiště (viz Použití funkce společného sledování úložiště) sleduje úložiště pod adresním prostorem MSTR jednotlivých správců front a lze ji použít ke zjištění, kolik prostoru globální moduly využívají.

Standardně jsou globální moduly v zaváděcí knihovně SCSQAUTH. Pokud adresní prostor MSTR správce front vyhledá SCSQAUTH prostřednictvím zřetězení STEPLIB, budou globální moduly z tohoto místa použity přednostně před libovolným modulem LPA a budou načteny do ECSA.

Globální moduly jsou:

CSQ0GPLM, CSQ3AMGP, CSQ3SSGP, CSQ9PREP,
CSQ9SCNB, CSQGGPLM, CSQMCGLM, CSQMGPLM, CSQRGLM1,
CSQSLD1, CSQVGEPL, CSQVSRX, CSQWDLD2, CSQWDLD3,
CSQWVZSA, CSQWZDG0, CSQWVZPS, CSQWVGTM, CSQZTDDM

Důležité:

- Název globálních modulů pro produkt IBM MQ zůstává konstantní napříč různými verzemi produktu IBM MQ . Pokud tedy načtete globální moduly do LPA, měly by být z jedné verze produktu IBM MQ a měly by být používány pouze správci front spuštěnými ve stejné verzi produktu IBM MQ .
- Je-li ve stejné oblasti LPAR spuštěno více verzí produktu IBM MQ , pak pouze jeden z nich může mít v oblasti LPA v daném okamžiku své globální moduly.
- Pokud je údržba použita na instalaci produktu IBM MQ , která má globální moduly načtené do LPA, a tato údržba aktualizuje některý z globálních modulů, měli byste znovu provést postup popsaný v následujícím textu.

Postup

Chcete-li vložit globální moduly z verze produktu IBM MQ do LPA, postupujte takto:

1. Vytvořte kopii zaváděcí knihovny `thlqual.SCSQAUTH` a jejího obsahu, například: `thlqual.LOCAL.SCSQAUTH`. Ujistěte se, že je tato zaváděcí knihovna chráněna před neoprávněným přístupem pomocí externího správce zabezpečení (ESM).
2. Autorizace APF pro zaváděcí knihovnu `thlqual.LOCAL.SCSQAUTH` ; viz “Autorizace APF pro zaváděcí knihovny IBM MQ” na stránce 878.
3. Vytvořte novou zaváděcí knihovnu `thlqual.GLOBAL.SCSQAUTH` se stejnými atributy jako `thlqual.LOCAL.SCSQAUTH`.

   Poznámka: Tato zaváděcí knihovna nemusí mít oprávnění APF. Ujistěte se, že je tato zaváděcí knihovna chráněna před neoprávněným přístupem pomocí ESM.
4. Zkopírujte 19 globálních modulů z adresáře `thlqual.LOCAL.SCSQAUTH` do adresáře `thlqual.GLOBAL.SCSQAUTH`.
5. Odstraňte 19 globálních modulů z adresáře `thlqual.LOCAL.SCSQAUTH`.
6. Umístěte 19 globálních modulů z `thlqual.GLOBAL.SCSQAUTH` do LPA, buď:
   a. a. Přidání `thlqual.GLOBAL.SCSQAUTH` do LPALSTxx člena SYS1.PARMLIB. Poté musíte provést IPL systému s volbou CLPA, abyste se ujistili, že obsah knihovny je načten do PLPA.
   b. b. Dynamické přidávání modulů do LPA pomocí následujícího příkazu:

```
SETPROG
LPA,ADD,MODNAME=(CSQ0GPLM,CSQ3AMGP,CSQ3SSGP,CSQ9PREP,CSQ9SCNB,CSQGGPLM,
CSQMCGLM,CSQMGPLM,CSQRGLM1,CSQSLD1,CSQVGEPL,CSQVSRX,CSQWDLD2,CSQWDLD3,
CSQWVZSA,CSQWZDG0,CSQWVZPS,CSQWVGTM,CSQZTDDM),DSNAME= thlqual.GLOBAL.SCSQAUTH
```

   Poznámka: LPALSTxx je preferovaný dlouhodobý způsob umístění modulů do LPA.
7. Ověřte, že jsou moduly v LPA, zadáním následujícího příkazu:

```
D PROG,LPA,MODNAME=CSQMCGLM
```

Výstup příkazu by měl indikovat vstupní a zaváděcí body modulu, pokud byl úspěšně načten do LPA.

Pro každého správce front, který potřebuje používat globální moduly z LPA, pak, pokud obvykle umísťujete:

1. `thlqual.SCSQAUTH` v seznamu odkazů, jen zastavte a spusťte svého správce front. Globální moduly se načítají z LPA a lokální moduly ze seznamu odkazů.
2. `thlqual.SCSQAUTH` v souboru JCL MSTR STEPLIB změňte soubor JCL tak, aby soubor STEPLIB používal místo souboru `thlqual.SCSQAUTH`hodnotu `thlqual.LOCAL.SCSQAUTH` . Zastavte a spusťte správce front; globální moduly jsou načteny z LPA a lokální moduly z STEPLIB.

Kód JCL CHIN a AMSM mohou i nadále používat `thlqual.SCSQAUTH` stejně jako libovolné aplikace IBM MQ .

Chcete-li vrátit zpět správce front k načtení globálních modulů do ECSA, postupujte takto:

1. Zastavit správce front
2. Odeberte globální moduly z LPA, buď při příštím IPL tak, že odeberete definice `LPALSTxx` , nebo pomocí následujícího příkazu:

```
SETPROG LPA,DELETE,MODNAME=(xxx) FORCE=YES
```

3. Pokud se soubor `thlqual.LOCAL.SCSQAUTH` nachází v knihovně STEPLIB správce front, nahraďte jej hodnotou `thlqual.SCSQAUTH`.
4. Restartujte správce front.

Související pojmy

“Aktualizovat seznam odkazů z/OS a LPA” na stránce 879
Aktualizujte knihovny LPA pomocí nové verze knihoven raného kódu. Další kód může jít v seznamu odkazů nebo LPA.

z/OS *Aktualizovat tabulku vlastností programu z/OS*

Pro správce front IBM MQ jsou zapotřebí některé další položky PPT.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že nastavení pro IBM MQ jsou identická na každém systému z/OS v prostředí sysplex.*
- *Tuto úlohu nemusíte provádět při migraci z předchozí verze.*
- *Musíte provést část CSQ0DSRV této úlohy, když požadujete Advanced Message Security.*

Ukázka obsahující všechny požadované položky PPT je uvedena v souboru thlqual.SCSQPROC(CSQ4SCHD). Ujistěte se, že jsou požadované položky přidány do tabulky PPT, kterou najdete v SYS1.PARMLIB(SCHEDxx).

V produktu z/OSje oblast CSQYASCP již pro operační systém definována s podrobnými atributy a již není nutné ji zahrnout do člena SCHEDxx knihovny PARMLIB.

Správce front IBM MQ řídí vlastní výměnu. Máte-li však silně zatíženou síť IBM MQ a doba odezvy je kritická, může být výhodné nastavit inicializátor kanálu IBM MQ jako nepřenositelný přidáním položky CSQXJST PPT s rizikem ovlivnění výkonu zbytku systému z/OS .

Pokud požadujete Advanced Message Security, přidejte položku PPT CSQ0DSRV .

Zadejte z/OS příkaz **SET SCH=xx**, kde *xx* je přípona člena SCHEDxx PARMLIB, aby se tyto změny projevily.

Související pojmy

“Definujte subsystém IBM MQ pro z/OS .” na stránce 884
Aktualizujte tabulku názvů subsystému a rozhodněte o konvenci pro řetězce předpon příkazů.

z/OS Konfigurace správce front a inicializátoru kanálu

Tato témata použijte jako průvodce krok za krokem pro konfiguraci správce front a inicializátoru kanálu.

z/OS *Definujte subsystém IBM MQ pro z/OS .*

Aktualizujte tabulku názvů subsystému a rozhodněte o konvenci pro řetězce předpon příkazů.

Tuto úlohu opakujte pro všechny správce front IBM MQ . Tuto úlohu nemusíte provádět při migraci z předchozí verze.

Související pojmy

“Vytvořit procedury pro správce front IBM MQ” na stránce 887
Každý subsystém IBM MQ potřebuje ke spuštění správce front katalogizovanou proceduru. Můžete vytvořit vlastní knihovnu procedur dodanou s produktem IBMnebo ji použít.

z/OS *Aktualizace tabulky názvů subsystémů*

Při definování subsystému IBM MQ musíte přidat záznam do tabulky názvů subsystémů.

Tabulka názvů subsystémů z/OS, která je na počátku převzata z SYS1.PARMLIB člen IEFSSNss, obsahuje definice formálně definovaných subsystémů z/OS . Chcete-li definovat každý subsystém IBM MQ , musíte do této tabulky přidat záznam, a to buď změnou člena IEFSSNss systému SYS1.PARMLIB, nebo nejlépe pomocí příkazu z/OS SETSSI.

Inicializace subsystému IBM MQ podporuje paralelní zpracování, takže příkazy definice subsystému IBM MQ lze přidat jak nad, tak pod klíčové slovo BEGINPARALLEL v tabulce IEFSSNss, která je k dispozici na adrese z/OS V1.12 a novější.

Pokud použijete příkaz SETSSI, změna se projeví okamžitě a není třeba provádět IPL vašeho systému. Ujistěte se, že aktualizujete SYS1.PARMLIB také, jak je popsáno v tématu “Aktualizujte SYS1.PARMLIB” na stránce 891 , aby změny zůstaly v platnosti i po následných IPL.

Příkaz SETSSI pro dynamické definování subsystému IBM MQ je:

```
SETSSI ADD,S=ssid,I=CSQ3INI,P='CSQ3EPX,cpf,scope'
```

Odpovídající informace v IEFSSNss lze zadat jedním ze dvou způsobů:

- Forma parametru klíčového slova definice subsystému IBM MQ v IEFSSNss. Jedná se o doporučenou metodu.

  ```
  SUBSYS SUBNAME(ssid) INITRTN(CSQ3INI) INITPARM('CSQ3EPX,cpf,scope')
  ```

- Forma pozičního parametru definice subsystému IBM MQ .

  ```
  ssid,CSQ3INI,'CSQ3EPX,cpf,scope'
  ```

Nemíchejte tyto dva formuláře v jednom členu IEFSSNss. Pokud jsou vyžadovány různé formuláře, použijte pro každý typ samostatný člen IEFSSNss a přidejte operand SSN nového člena do IEASYSpp SYS1.PARMLIB . Chcete-li zadat více než jedno SSN, použijte SSN = (aa, bb, ...) v IEASYSpp.

V příkladech

ssid
: Identifikátor subsystému. Může mít délku až čtyři znaky. Všechny znaky musí být alfanumerické (velká písmena A až Z, 0 až 9), musí začínat abecedním znakem. Správce front bude mít stejný název jako subsystém, proto můžete použít pouze znaky, které jsou povoleny pro názvy objektů z/OS i IBM MQ .

cpf
Řetězec předpony příkazu (informace o CPF viz “Definování řetězců předpon příkazů (CPFs)” na stránce 885).

scope
Rozsah systému, který se používá, pokud pracujete v prostředí sysplex systému z/OS (informace o rozsahu systému viz “CPF v prostředí prostředí sysplex” na stránce 886).

Obrázek 100 na stránce 885 ukazuje několik příkladů příkazů IEFSSNss.

```
CSQ1,CSQ3INI,'CSQ3EPX,+mqs1cpf,S'
CSQ2,CSQ3INI,'CSQ3EPX,+mqs2cpf,S'
CSQ3,CSQ3INI,'CSQ3EPX,++,S'
```

Obrázek 100. Ukázkové příkazy IEFSSNss pro definování subsystémů

Poznámka: Když jste vytvořili objekty v subsystému, nemůžete změnit název subsystému nebo použít sady stránek z jednoho subsystému v jiném subsystému. Chcete-li provést některou z těchto akcí, musíte uvolnit všechny objekty a zprávy z jednoho subsystému a znovu je načíst do jiného.

Tabulka 54 na stránce 885 uvádí řadu příkladů, které zobrazují přidružení názvů subsystémů a řetězců předpon příkazů (CPF), jak jsou definovány příkazy v souboru Obrázek 100 na stránce 885.

Tabulka 54. Název subsystému pro přidružení CPF

IBM MQ název subsystému	**CPF**
CSQ1	+mqs1cpf
CSQ2	+mqs2cpf
CSQ3	++

Poznámka: Funkce ACTIVATE a DEACTIVATE příkazu z/OS SETSSI nejsou produktem IBM MQpodporovány.

Chcete-li zkontrolovat stav změn, zadejte v souboru SDSFnásledující příkaz: `/D SSI,L`. Uvidíte nové subsystémy vytvořené ve stavu AKTIVNÍ.

z/OS *Definování řetězců předpon příkazů (CPFs)*

Každá instance subsystému IBM MQ může mít řetězec předpony příkazu k identifikaci tohoto subsystému.

Přijměte celosystémovou konvenci pro vaše CPF pro všechny subsystémy, abyste se vyhnuli konfliktům. Dodržujte následující pokyny:

- Definujte CPF jako řetězec o délce až osm znaků.
- Nepoužívejte CPF, který je již používán jiným subsystémem, a nepoužívejte znak JES backspace definovaný v systému jako první znak vašeho řetězce.
- Definujte CPF pomocí znaků ze sady platných znaků uvedených v části Tabulka 56 na stránce 886.
- Nepoužívejte funkci CPF, která je zkratkou pro již definovaný proces, nebo která by mohla být zaměněna se syntaxí příkazu. Například CPF, jako např. 'D', je v konfliktu s příkazy z/OS , jako např. DISPLAY. Chcete-li se tomu vyhnout, použijte jeden ze speciálních znaků (viz Tabulka 56 na stránce 886). jako první nebo jediný znak v řetězci CPF.
- Nedefinujte CPF, který je buď podmnožinou, nebo nadřazenou sadou existujícího CPF. Příklad viz Tabulka 55 na stránce 885.

Tabulka 55. Příklad pravidel podmnožiny CPF a supersady

Název subsystému	**Definice CPF**	**Příkazy směrovány na**
MQA	!A	MQA

Tabulka 55. Příklad pravidel podmnožiny CPF a supersady (pokračování)		
Název subsystému	**Definice CPF**	**Příkazy směrovány na**
MQB	!B	MQB
MQC1	!C1	MQC1
MQC2	!C2	MQC2
MQB1	!B1	MQB

Příkazy určené pro subsystém MQB1 (s použitím CPF!B1) jsou směrovány do subsystému MQB, protože CPF pro tento subsystém je!B, podmnožina!B1. Pokud jste například zadali příkaz:

```
!B1  START  QMGR
```

subsystém MQB přijímá příkaz:

```
1 START QMGR
```

(které se v tomto případě nemůže zabývat).

Pomocí příkazu z/OS DISPLAY OPDATA můžete zjistit, které předpony existují.

Pokud pracujete v prostředí sysplex, produkt z/OS diagnostikuje jakékoli konflikty tohoto typu v době registrace CPF (informace o registraci CPF naleznete v části “CPF v prostředí prostředí sysplex” na stránce 886).

Tabulka 56 na stránce 886 zobrazuje znaky, které můžete použít při definování řetězců CPF:

Tabulka 56. Platná znaková sada pro řetězce CPF	
Znaková sada	**Obsah**
Abecední	Velká písmena A až Z, malá písmena a až z
Číselné	0 až 9
Národní (viz poznámka)	@ $# (Znaky, které lze reprezentovat jako hexadecimální hodnoty)
Speciální	. □ ( ) * & + - = ¢ < | ! ; % _ ? : >

Poznámka:

Systém rozpoznává následující hexadecimální reprezentace národních znaků: @ jako X'7C', $jako X'5B' a # jako X'7B'. V jiných zemích než U.S. U.S. národní znaky reprezentované na klávesnicích terminálu mohou generovat jinou hexadecimální reprezentaci a způsobit chybu. Například v některých zemích může znak $generovat znak X'4A'.

Středník (;) je platný jako CPF, ale na většině systémů je tento znak oddělovačem příkazů.

z/OS *CPF v prostředí prostředí sysplex*

V tomto tématu se dozvíte, jak používat funkce CPF v rámci prostředí sysplex.

Pokud se používá v prostředí sysplex, produkt IBM MQ zaregistruje vaše CPF, aby vám umožnil zadat příkaz z libovolné konzoly v prostředí sysplex a směrovat tento příkaz do příslušného systému pro provedení. Odezvy příkazu jsou vráceny do původní konzoly.

Definování rozsahu pro operaci prostředí sysplex

Rozsah se používá k určení typu registrace CPF prováděné subsystémem IBM MQ při spuštění produktu IBM MQ v prostředí sysplex.

Možné hodnoty pro rozsah jsou následující:

M

Rozsah systému.

CPF je registrován v produktu z/OS v době IPL systému produktem IBM MQ a zůstává registrován po celou dobu, kdy je systém z/OS aktivní.

Příkazy IBM MQ musí být zadány na konzole připojené k obrazu z/OS , na kterém běží cílový subsystém, nebo musíte použít příkazy ROUTE k přesměrování příkazu na tento obraz.

Tuto volbu použijte, pokud nejste spuštěni v prostředí sysplex.

S

Prostředí sysplex spustilo rozsah.

CPF je registrován v systému z/OS při spuštění subsystému IBM MQ a zůstává aktivní, dokud se subsystém IBM MQ neukončí.

K přesměrování původního příkazu START QMGR na cílový systém musíte použít příkazy ROUTE, ale všechny další příkazy IBM MQ lze zadat na libovolné konzole připojené k prostředí sysplex a jsou automaticky směrovány na cílový systém.

Po ukončení IBM MQ musíte použít příkazy ROUTE k nasměrování následných příkazů START do cílového subsystému IBM MQ .

X

Rozsah IPL prostředí sysplex.

CPF je registrován v produktu z/OS v době IPL systému produktem IBM MQ a zůstává registrován po celou dobu, kdy je systém z/OS aktivní.

Příkazy systému IBM MQ lze zadat v libovolné konzole připojené k prostředí sysplex a jsou směrovány do obrazu, který automaticky spouští cílový systém.

Subsystém IBM MQ s CPF s rozsahem S může být definován na jednom nebo více obrazech z/OS v prostředí sysplex, takže tyto obrazy mohou sdílet jednu tabulku názvů subsystému. Musíte se však ujistit, že počáteční příkaz START je vydán na (nebo směrován na) obraz z/OS , na kterém chcete spustit subsystém IBM MQ . Pokud použijete tuto volbu, můžete zastavit subsystém IBM MQ a restartovat jej na jiném obrazu systému z/OS v prostředí sysplex, aniž byste museli změnit tabulku názvů subsystému nebo provést IPL systému z/OS .

Subsystém IBM MQ s CPF s rozsahem X lze definovat pouze na jednom obrazu z/OS v prostředí sysplex. Použijete-li tuto volbu, musíte definovat jedinečnou tabulku názvů subsystémů pro každý z/OS obraz vyžadující IBM MQ subsystémy s CPF rozsahu X.

Chcete-li použít z/OS správce automatického restartu (ARM) k automatickému restartování správců front v různých obrazech z/OS , musí být každý správce front definován v každém obrazu produktu z/OS , v němž může být daný správce front restartován. Každý správce front musí být definován s jedinečným 4znakovým názvem subsystému v rámci prostředí sysplex s rozsahem CPF S.

z/OS *Vytvořit procedury pro správce front IBM MQ*

Každý subsystém IBM MQ potřebuje ke spuštění správce front katalogizovanou proceduru. Můžete vytvořit vlastní knihovnu procedur dodanou s produktem IBMnebo ji použít.

- Tuto úlohu opakujte pro všechny správce front IBM MQ .
- Při migraci z předchozí verze může být nutné katalogizovanou proceduru upravit.

Pro každý subsystém IBM MQ definovaný v tabulce názvů subsystému vytvořte v knihovně procedur katalogizovanou proceduru pro spuštění správce front. Knihovna procedur dodaná IBMse nazývá SYS1.PROCLIB, ale vaše instalace může používat vlastní konvenci pojmenování.

Název procedury spuštěné úlohy správce front je tvořen zřetězením názvu subsystému se znaky MSTR. Například subsystém CSQ1 má název procedury CSQ1MSTR. Pro každý subsystém, který definujete, potřebujete jednu proceduru.

Musíte zahrnout knihovnu obsahující zprávy ve vybraném jazyce:

- thlqual.SCSQSNLE, pro anglickou smíšenou velikost písmen
- thlqual.SCSQSNLU, pro americkou angličtinu velká písmena
- thlqual.SCSQSNLK, pro japonštinu
- thlqual.SCSQSNLF, pro francouzštinu
- thlqual.SCSQSNLC, pro čínštinu

Mnoho příkladů a pokynů v této dokumentaci produktu předpokládá, že máte subsystém s názvem CSQ1. Tyto příklady můžete snáze použít, pokud je na počátku vytvořen subsystém s názvem CSQ1 pro účely ověření instalace a testování.

V souboru thlqual.SCSQPROCjsou k dispozici dvě ukázkové procedury spuštěných úloh. Člen CSQ4MSTR používá jednu sadu stránek pro každou třídu zprávy. Člen CSQ4MSRR používá pro hlavní třídy zpráv více sad stránek. Zkopírujte jednu z těchto procedur do členu xxxxMSTR (kde xxxx je název vašeho subsystému IBM MQ) vašeho SYS1.PROCLIB nebo, pokud nepoužíváte SYS1.PROCLIB, vaše knihovna procedur. Zkopírujte ukázkovou proceduru do členu v knihovně procedur pro každý subsystém IBM MQ , který definujete.

Po zkopírování členů je můžete přizpůsobit požadavkům jednotlivých subsystémů podle pokynů v daném členu. Informace o určení omezení úložiště používaného správcem front naleznete v tématu Konfigurace úložiště. Můžete také použít symbolické parametry v JCL, chcete-li povolit úpravu procedury při jejím spuštění. Máte-li několik subsystémů IBM MQ , může být pro zjednodušení budoucí údržby výhodné používat pro společné části procedury skupiny zahrnutí JCL.

Používáte-li skupiny sdílení front, musí zřetězení STEPLIB obsahovat cílovou knihovnu běhového prostředí Db2 SDSNLOAD a musí mít autorizaci APF. Tato knihovna je ve zřetězení STEPLIB vyžadována pouze v případě, že není přístupná prostřednictvím seznamu odkazů nebo LPA.

Notes:

1. Můžete si poznamenat názvy své datové sady samozavedení (BSDS), protokolů a sad stránek pro použití v JCL a poté tyto sady definovat v pozdějším kroku procesu.
2. Ukázkové procedury spuštěných úloh CSQ4MSTR a CSQ4MSRR byly aktualizovány tak, aby zahrnovaly kartu CSQMINI DD, kterou lze použít k definování datové sady QMINI obsahující zabezpečení transportu, tj. vlastnosti zabezpečení SSL nebo TLS, s komentářem.

   Pomocí produktu “Datová sada QMINI” na stránce 894 můžete povolit nebo zakázat podporu TLS 1.3 anebo jej můžete použít k definování vlastního seznamu CipherSpecs , které mají kanály používat.

Související pojmy

“Vytvořit procedury pro inicializátor kanálu” na stránce 888
Pro každý subsystém IBM MQ upravte kopii souboru CSQ4CHIN. V závislosti na tom, jaké další produkty používáte, možná budete muset povolit přístup k jiným datovým sadám.

z/OS *Vytvořit procedury pro inicializátor kanálu*

Pro každý subsystém IBM MQ upravte kopii souboru CSQ4CHIN. V závislosti na tom, jaké další produkty používáte, možná budete muset povolit přístup k jiným datovým sadám.

- Tuto úlohu opakujte pro všechny správce front IBM MQ .
- Při migraci z předchozí verze může být nutné katalogizovanou proceduru upravit.

Je třeba vytvořit proceduru spuštění inicializátoru kanálu pro každý subsystém IBM MQ , který bude používat distribuované řazení do front.

Postupujte takto:

1. Zkopírujte ukázkovou proceduru spuštěné úlohy thlqual.SCSQPROC(CSQ4CHIN) do knihovny procedur. Pojmenujte proceduru *xxxx* CHIN, kde *xxxx* je název vašeho subsystému IBM MQ (například CSQ1CHIN bude procedura úlohy spuštěné inicializátorem kanálu pro správce front CSQ1).
2. Vytvořte kopii pro každý subsystém IBM MQ , který budete používat.
3. Přizpůsobte procedury vašim požadavkům pomocí pokynů v ukázkové proceduře CSQ4CHIN. Můžete také použít symbolické parametry v JCL, chcete-li povolit úpravu procedury při jejím spuštění. Toto je popsáno s volbami spuštění v části Administrace IBM MQ for z/OS.

   Zřetězení distribuované knihovny front thlqual.SCSQMVR1.

   Je vyžadován přístup ke knihovně běhového prostředí LE SCEERUN; pokud není ve vašem seznamu odkazů (SYS1.PARMLIB(LNKLSTkk)), zřetězte jej v příkazu STEPLIB DD.

   V 9.3.1 Zvažte úpravu parametru MEMLIMIT pomocí informací v části Konfigurace úložiště.
4. Autorizujte procedury ke spuštění pod vaším externím správcem zabezpečení.
5. Musíte zahrnout knihovnu obsahující zprávy ve vybraném jazyce:
   - thlqual.SCSQSNLE, pro anglickou smíšenou velikost písmen
   - thlqual.SCSQSNLU, pro americkou angličtinu velká písmena
   - thlqual.SCSQSNLK, pro japonštinu
   - thlqual.SCSQSNLF, pro francouzštinu
   - thlqual.SCSQSNLC, pro čínštinu

Inicializátor kanálu je dlouhotrvající adresní prostor. Chcete-li zabránit jeho ukončení poté, co bylo spotřebováno omezené množství CPU, potvrďte, že:

- Výchozí hodnota pro spuštěné úlohy v systému z/OS je neomezená hodnota CPU. Toto je dosaženo pomocí konfiguračního příkazu JES2 pro parametr JOBCLASS (STC) s hodnotou TIME = (1440,00).
- Explicitně přidejte parametr TIME=1440nebo TIME=NOLIMIT do příkazu EXEC pro CSQXJST.

Chcete-li použít uživatelské procedury kanálu, můžete do této procedury přidat knihovnu uživatelských procedur (CSQXLIB) později. Chcete-li to provést, musíte zastavit a restartovat inicializátor kanálu.

Používáte-li protokol TLS, je vyžadován přístup k běhové knihovně systémového protokolu TLS. Tato knihovna se nazývá SIEALNKE. Knihovna musí mít oprávnění APF.

Používáte-li protokol TCP/IP, musí být adresní prostor inicializátoru kanálu schopen přistupovat k protokolu TCPIP.DATA , která obsahuje parametry systému TCP/IP. Způsob, jakým má být datová sada nastavena, závisí na tom, který produkt TCP/IP a rozhraní používáte. Mezi ně patří:

- Proměnná prostředí, RESOLVER_CONFIG
- /etc/resolv.conf v systému souborů
- // Příkaz SYSTCPD DD
- // Příkaz SYSTCPDD DD
- *jobname/userid*.TCPIP.DATA
- SYS1.TCPPARMS(TCPDATA)
- *zapname*.TCPIP.DATA

Některé z nich ovlivňují váš skript JCL procedury spuštěných úloh. Další informace naleznete v příručce z/OS Communications Server: IP Configuration Guide.

Související pojmy

“Definovat subsystém IBM MQ pro třídu služeb WLM systému z/OS” na stránce 890

Chcete-li udělit IBM MQ odpovídající prioritu výkonu v systému z/OS , musíte přiřadit adresní prostory správce front a inicializátoru kanálu příslušné třídě služeb WLM (z/OS Workload Management). Pokud tak neučiníte explicitně, mohou se použít nevhodná výchozí nastavení.

z/OS *Definovat subsystém IBM MQ pro třídu služeb WLM systému z/OS*

Chcete-li udělit IBM MQ odpovídající prioritu výkonu v systému z/OS , musíte přiřadit adresní prostory správce front a inicializátoru kanálu příslušné třídě služeb WLM (z/OS Workload Management). Pokud tak neučiníte explicitně, mohou se použít nevhodná výchozí nastavení.

- *Tuto úlohu opakujte pro každého IBM MQ správce front.*
- *Tuto úlohu nemusíte provádět při migraci z předchozí verze.*

Dialogové okno ISPF dodávané se správcem WLM použijte k provedení následujících úloh:

- Extrahujte definici zásady WLM z/OS z datové sady dvojice WLM.
- Aktualizovat tuto definici zásady přidáním názvů procedur spuštěných úloh správce front a inicializátoru kanálu do zvolené třídy služeb
- Instalovat změněnou zásadu do datové sady dvojice WLM

Pak aktivujte tuto zásadu pomocí příkazu z/OS

```
V WLM,POLICY=policyname,REFRESH
```

Další informace o nastavení voleb výkonu viz Plánování prostředí IBM MQ na z/OS .

Související pojmy

“Nastavení prostředí Db2” na stránce 927
Pokud používáte skupiny sdílení front, musíte vytvořit požadované objekty Db2 úpravou a spuštěním řady ukázkových úloh.

z/OS *Implementace ovládacích prvků zabezpečení ESM*

Implementujte řízení zabezpečení pro správce front a iniciátor kanálu.

- *Tuto úlohu opakujte pro každého IBM MQ správce front.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*

Používáte-li produkt RACF jako svého externího správce zabezpečení, přečtěte si téma Nastavení zabezpečení v systému z/OS , které popisuje, jak implementovat tyto ovládací prvky zabezpečení.

Používáte-li inicializátor kanálu, musíte také provést následující akce:

- Má-li váš subsystém aktivní zabezpečení připojení, definujte profil zabezpečení připojení ssid.CHIN pro vašeho externího správce zabezpečení (informace o tom naleznete v tématu Profily zabezpečení připojení pro inicializátor kanálu).
- Používáte-li protokol TLS (Transport Layer Security) nebo rozhraní soketů, ujistěte se, že ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je nakonfigurováno pro použití produktu z/OS UNIX System Services, jak je popsáno v dokumentaci *z/OS UNIX System Services Plánování* .
- Používáte-li protokol TLS, ujistěte se, že ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je konfigurováno pro přístup ke svazku klíčů zadanému v parametru SSLKEYR příkazu ALTER QMGR.

Před spuštěním správce front nastavte datovou sadu IBM MQ a zabezpečení systému takto:

- Autorizace správce front spustila proceduru úlohy, která se má spustit pod vaším externím správcem zabezpečení.
- Autorizace přístupu k datovým sadám správce front.
- Konfigurace šifrování datové sady z/OS , je-li požadováno.

Viz část důvěrnost pro data v klidu na systému IBM MQ for z/OS se šifrováním datové sady. Další informace viz.

Podrobnosti o tom, jak to provést, naleznete v tématu Úlohy instalace zabezpečení pro produkt z/OS.

Používáte-li produkt RACF, za předpokladu, že používáte třídu RACF STARTED, nemusíte provádět IPL svého systému (viz RACF autorizace procedur spuštěných úloh).

Související pojmy

“Aktualizujte SYS1.PARMLIB” na stránce 891
Chcete-li se ujistit, že vaše změny zůstanou v platnosti i po IPL, musíte aktualizovat některé členy SYS1.PARMLIB

“Implementace ovládacích prvků zabezpečení ESM pro skupinu sdílení front” na stránce 930
Implementujte řízení zabezpečení pro všechny správce front ve skupině sdílení front pro přístup k produktu Db2 a strukturám seznamu prostředku Coupling Facility.

z/OS *Aktualizujte SYS1.PARMLIB*

Chcete-li se ujistit, že vaše změny zůstanou v platnosti i po IPL, musíte aktualizovat některé členy SYS1.PARMLIB

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že nastavení pro IBM MQ jsou identická na každém systému z/OS v prostředí sysplex.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*

Aktualizujte SYS1.PARMLIB jsou následující:

1. Aktualizujte člena IEFSSNss, jak je popsáno v tématu “Definujte subsystém IBM MQ pro z/OS .” na stránce 884.
2. Změňte IEASYSpp tak, aby při provádění IPL byly použity následující členy:
   - členy PROGxx nebo IEAAPFaa použité v “Autorizace APF pro zaváděcí knihovny IBM MQ” na stránce 878
   - členy LNKLSTkk a LPALSTmm použité v “Aktualizovat seznam odkazů z/OS a LPA” na stránce 879
   - člen SCHEDxx použitý v adresáři “Aktualizovat tabulku vlastností programu z/OS” na stránce 883
   - člen IEFSSNss použitý v “Definujte subsystém IBM MQ pro z/OS .” na stránce 884

Související pojmy

“Upravit vstupní datové sady inicializace” na stránce 891
Vytvořte pracovní kopie ukázkových vstupních datových sad inicializace a přizpůsobte je tak, aby vyhovovaly vašim systémovým požadavkům.

z/OS *Upravit vstupní datové sady inicializace*

Vytvořte pracovní kopie ukázkových vstupních datových sad inicializace a přizpůsobte je tak, aby vyhovovaly vašim systémovým požadavkům.

- *Tuto úlohu opakujte pro každého IBM MQ správce front.*
- *Tuto úlohu musíte provést při migraci z předchozí verze.*

Každý správce front IBM MQ získává své počáteční definice z řady příkazů obsažených v IBM MQ *vstupních datových sadách inicializace*. Na tyto datové sady odkazují názvy definic dat CSQINP1, CSQINP2a CSQINPT definované v proceduře spuštěné úlohy správce front.

Odpovědi na tyto příkazy se zapisují do datových sad výstupu inicializace, na které odkazují názvy definic dat CSQOUT1, CSQOUT2 a CSQOUTT.

Chcete-li zachovat originály, vytvořte pracovní kopie každého vzorku. Pak můžete příkazy v těchto pracovních kopiích upravit tak, aby vyhovovaly vašim systémovým požadavkům.

Pokud použijete více než jeden subsystém IBM MQ a název subsystému zahrnete do kvalifikátoru vyšší úrovně názvu vstupní datové sady inicializace, můžete snadněji identifikovat subsystém IBM MQ přidružený ke každé datové sadě.

Další informace o ukázkách naleznete v následujících tématech:

- Formáty inicializačních datových sad
- Použití ukázky CSQINP1
- Použití ukázek CSQINP2
- Použití ukázky CSQINPX
- Použití ukázky CSQINPT

Formáty inicializačních datových sad

Inicializační vstupní datové sady mohou být členy rozdělené datové sady (PDS) nebo sekvenční datové sady. Mohou být zřetězenou řadou datových sad. Definujte je s délkou záznamu 80 bajtů, kde:

- Významné jsou pouze sloupce 1 až 72. Sloupce 73 až 80 jsou ignorovány.
- Záznamy s hvězdičkou (*) ve sloupci 1 jsou interpretovány jako komentáře a jsou ignorovány.
- Prázdné záznamy jsou ignorovány.
- Každý příkaz musí být spuštěn na novém záznamu.
- Koncové-znamená pokračovat od sloupce 1 dalšího záznamu.
- Koncové znaménko + znamená pokračování od prvního neprázdného sloupce dalšího záznamu.
- Maximální povolený počet znaků v příkazu je 32 762.

Výstupní datové sady inicializace jsou sekvenční datové sady s délkou záznamu 125, formátem záznamu VBA a velikostí bloku 629.

Použití ukázky CSQINP1

Datová sada `thlqual.SCSQPROC` obsahuje dva členy, které obsahují definice fondů vyrovnávacích pamětí, sadu stránek pro přidružení fondů vyrovnávacích pamětí a příkaz ALTER SECURITY.

Člen CSQ4INP1 používá jednu sadu stránek pro každou třídu zprávy. Zprávy jsou rozděleny do následujících tříd:

- Zprávy související se systémem.
- Důležité zprávy s dlouhou životností.
- Krátkodobé zprávy.
- Různé zprávy.

Člen CSQ4INPR používá více sad stránek pro každou hlavní třídu zprávy a jednu sadu stránek pro každou jinou třídu. Následují hlavní třídy zpráv:

- Důležité zprávy s dlouhou životností.
- Krátkodobé zprávy.

Do zřetězení CSQINP1 procedury spuštěné úlohy správce front zahrňte příslušnou ukázku.

Notes:

1. Produkt IBM MQ podporuje až 100 fondů vyrovnávacích pamětí v rozsahu od 0 do 99. Příkaz DEFINE BUFFPOOL lze zadat pouze z datové sady inicializace CSQINP1 . Definice v ukázce určují čtyři fondy vyrovnávacích pamětí.
2. Každá sada stránek používaná správcem front musí být definována v datové sadě inicializace CSQINP1 pomocí příkazu DEFINE PSID. Definice sady stránek přidružuje ID fondu vyrovnávacích pamětí k sadě stránek. Není-li určen žádný fond vyrovnávacích pamětí, použije se standardně nulový fond vyrovnávacích pamětí.

Musí být definována sada stránek nula (00). Obsahuje všechny definice objektů. Pro každého správce front můžete definovat až 100 sad stránek.

3. Příkaz ALTER SECURITY lze použít ke změně atributů zabezpečení TIMEOUT a INTERVAL. V produktu CSQ4INP1jsou výchozí hodnoty definovány jako 54 pro TIMEOUT a 12 pro INTERVAL.

Informace o uspořádání fondů vyrovnávacích pamětí a sad stránek naleznete v tématu Plánování sad stránek a fondů vyrovnávacích pamětí .

Změníte-li fond vyrovnávacích pamětí a definice sad stránek dynamicky za běhu správce front, měli byste také aktualizovat definice CSQINP1 . Změny jsou zachovány pouze pro studený začátek IBM MQ, pokud definice fondu vyrovnávacích pamětí neobsahuje atribut REPLACE.

Použití ukázek CSQINP2

V této tabulce jsou uvedeny členy databáze `thlqual.SCSQPROC` , které lze zahrnout do zřetězení CSQINP2 vaší procedury spuštěné úlohy správce front s popisem jejich funkce. Konvence pojmenování je CSQ4IN*. CSQ4INY* členy by měly být upraveny pro vaši konfiguraci. Neměli byste měnit členy CSQINS*, protože při migraci na další verzi budete muset znovu použít všechny změny. Místo toho můžete vložit příkazy DEFINE nebo ALTER do členů CSQ4INY* .

Tabulka 57. Členové `thlqual.SCSQPROC`

Název člena	**Popis**
CSQ4INSG	Definice systémových objektů.
CSQ4INSA	Systémový objekt a výchozí pravidla pro ověřování kanálu.
CSQ4INSX	Definice systémových objektů.
CSQ4INSS	Pokud používáte skupiny sdílení front, upravte tohoto člena a začleňte jej.
CSQ4INSJ	Upravte a zahrňte tohoto člena, pokud používáte publikování/odběr pomocí JMS.
CSQ4INSM	Definice systémových objektů pro Advanced Message Security.
CSQ4INSR	Upravte a zahrňte tohoto člena, pokud používáte produkt WebSphere Application Server, nebo rozhraní pro publikování/odběr ve frontě podporované démonem publikování/odběru ve frontě v produktu IBM MQ.
CSQ4DISP	Ukázka CSQINP2 pro zobrazení definic objektů.
CSQ4INYC	Definice klastrování.
CSQ4INYD	Definice distribuovaných front.
CSQ4INYG	Obecné definice.
CSQ4INYR	Definice paměťových tříd s použitím více sad stránek pro hlavní třídy zpráv.
CSQ4INYS	Definice paměťových tříd s použitím jedné sady stránek pro každou třídu zpráv.

Objekty je třeba definovat pouze jednou, nikoli vždy, když spouštíte správce front, takže není nutné tyto definice vždy zahrnout do CSQINP2 . Pokud je zahrnete pokaždé, pokoušíte se definovat objekty, které již existují, a dostanete zprávy podobné následujícím:

```
CSQM095I +CSQ1 CSQMAQLC QLOCAL(SYSTEM.DEFAULT.LOCAL.QUEUE) ALREADY EXISTS
CSQM090E +CSQ1 CSQMAQLC FAILURE REASON CODE X'00D44003'
CSQ9023E +CSQ1 CSQMAQLC ' DEFINE QLOCAL' ABNORMAL COMPLETION
```

Objekty nejsou tímto selháním poškozeny. Chcete-li datovou sadu definic SYSTEM ponechat ve zřetězení CSQINP2 , můžete se vyhnout zprávám o selhání zadáním atributu REPLACE pro každý objekt.

Použití ukázky CSQINPX

Ukázka `thlqual.SCSQPROC(CSQ4INPX)` obsahuje sadu příkazů, které můžete chtít provést při každém spuštění inicializátoru kanálu. Jedná se obvykle o příkazy související s kanály, například START LISTENER, které jsou vyžadovány při každém spuštění inicializátoru kanálu, nikoli při každém spuštění správce front a které nejsou povoleny ve vstupních datových sadách CSQINP1 nebo CSQINP2. Tuto ukázku musíte před použitím upravit; poté ji můžete zahrnout do datové sady CSQINPX pro inicializátor kanálu.

Příkazy IBM MQ obsažené v datové sadě se provedou na konci inicializace inicializátoru kanálu a výstup se zapíše do datové sady uvedené příkazem CSQOUTX DD. Výstup je podobný výstupu vytvořeným funkcí COMMAND obslužného programu IBM MQ (CSQUTIL). Viz Použití obslužného programu CSQUTIL pro IBM MQ for z/OS.

Můžete zadat libovolný z příkazů IBM MQ , které lze zadat z knihovny CSQUTIL, nikoli pouze příkazy kanálu. Během zpracování CSQINPX můžete zadávat příkazy z jiných zdrojů. Všechny příkazy jsou vydávány postupně bez ohledu na úspěch předchozího příkazu.

Chcete-li určit dobu odezvy příkazu, můžete použít pseudopříkaz COMMAND jako první příkaz v datové sadě. To vyžaduje jedno volitelné klíčové slovo RESPTIME (*nnn*), kde *nnn* je doba v sekundách, po kterou se má čekat na odpověď na každý příkaz. Toto je v rozsahu 5 až 999; předvolba je 30.

Pokud produkt IBM MQ zjistí, že odezvy na čtyři příkazy trvaly příliš dlouho, zpracování modulu CSQINPX se zastaví a nebudou vydány žádné další příkazy. Inicializátor kanálu není zastaven, ale do datové sady CSQOUTX je zapsána zpráva CSQU052E a na konzolu je odeslána zpráva CSQU013E .

Když produkt IBM MQ úspěšně dokončí zpracování CSQINPX, na konzolu se odešle zpráva CSQU012I .

Použití ukázky CSQINPT

V této tabulce jsou uvedeny členy databáze `thlqual.SCSQPROC` , které lze zahrnout do zřetězení CSQINPT procedury spuštěné úlohy vašeho správce front, s popisem jejich funkce.

Tabulka 58. Členové `thlqual.SCSQPROC`	
Název člena	**Popis**
CSQ4INST	Výchozí definice odběru systému.
CSQ4INYT	Definice publikování/odběru.

Příkazy IBM MQ obsažené v datové sadě se provedou po dokončení inicializace publikování/odběru a výstup se zapíše do datové sady uvedené příkazem CSQOUTT DD. Výstup je podobný výstupu vytvořeným funkcí COMMAND obslužného programu IBM MQ (CSQUTIL). Viz Použití obslužného programu CSQUTIL pro IBM MQ for z/OS.

Související pojmy

“Vytvořit datové sady zaváděcího programu a protokolu” na stránce 896
Pomocí dodaného programu CSQJU003 připravte datové sady zaváděcího programu (BSDS) a datové sady protokolu.

z/OS *Datová sada QMINI*

Datovou sadu QMINI můžete použít k určení vlastností, které mají být načteny a zpracovány během inicializace správce front.

Charakteristika datové sady QMINI

Datová sada QMINI je sekvenční datová sada nebo člen dělené datové sady s maximální délkou záznamu 80 bajtů (72 bajtů pro data a osm bajtů pro číslo řádku).

Následující příklad ukazuje vlastnosti pro sekvenční datovou sadu QMINI. Některé vlastnosti jsou samozřejmě založeny na vašem prostředí.

```
Data Set Name . . . . : QM01.QMINI
General Data                          Current Allocation
Management class . .  : STANDARD      Allocated tracks  . : 1
Storage class  . . .  : STANDARD      Allocated extents . : 1
Volume serial . . .   : P5P21E
Device type . . . .   : 3390
Data class . . . . .  : **None**
Organization  . . .   : PS            Current Utilization
Record format . . .   : FB            Used tracks . . . . : 0
Record length . . .   : 80            Used extents  . . . : 0
Block size  . . . .   : 3120
1st extent tracks .   : 1
Secondary tracks  .   : 1             Dates
Data set name type    :               Creation date . . . : 2020/08/11
Data set encryption   : NO            Referenced date . . : ***None***
                                      Expiration date . . : ***None***
SMS Compressible  .   : NO
```

`thlqual.SCSQPROC`, zahrnuje:

- Ukázkový obsah pro datovou sadu QMINI v CSQ4QMIN.
- Příklad určení datové sady QMINI pomocí karty // CSQMINI DD v JCL spuštění správce front v procedurách spuštěných úloh CSQ4MSTR a CSQ4MSRR.

Notes:

- Kód, který analyzuje datovou sadu, analyzuje pouze prvních 72 bajtů každého záznamu.
- Čísla řádků se ignorují, takže není nutné uvádět čísla řádků.
- Pokud řádek začíná znakem hvězdičky (*), je považován za komentář.
- Obsah datové sady QMINI je analyzován během spuštění správce front. Pokud je obsah úspěšně analyzován, je v protokolu úloh správce front vydána zpráva CSQM578I . Dojde-li během analýzy k chybám, budou v protokolu úloh správce front vydány chybové zprávy, například CSQM573E, ale správce front bude stále spuštěn.

  Zkontrolujte chybové zprávy a vyřešte případné problémy v obsahu datové sady QMINI.

  Pokud správce front nemůže analyzovat datovou sadu QMINI, můžete spustit inicializátor kanálu, ale nemůžete spustit žádné kanály, které jsou konfigurovány pro použití zabezpečení SSL nebo TLS, protože nastavení konfigurace zabezpečení jsou neznámá.
- Pokud provedete jakékoli aktualizace datové sady po spuštění správce front, musíte restartovat správce front, aby se změny projevily.

Sekce TransportSecurity

V produktu IBM MQ for z/OS 9.2.0datová sada QMINI podporuje sekci `TransportSecurity` . Tato sekce poskytuje podobnou funkci, jakou poskytuje sekce SSL v souboru qm.ini na systému IBM MQ for Multiplatforms.

Sekce `TransportSecurity` podporuje následující vlastnosti:

AllowTLSV13
Zda může správce front používat protokol TLS 1.3 CipherSpecs; platné hodnoty jsou: *TRUE/T/YES/Y* nebo *FALSE/F/NO/N*.

Pro migrované správce front není standardně povoleno zabezpečení TLS 1.3 . Protokol TLS 1.3 můžete povolit definováním datové sady QMINI pomocí sekce `TransportSecurity` a **`AllowTLSV13`**=TRUE.

Pro nově vytvořené správce front je standardně povoleno zabezpečení TLS 1.3 .

Specifikace AllowedCipher
Vlastní seznam CipherSpecs , které jsou povoleny.

Další informace o této vlastnosti naleznete v tématu Poskytnutí vlastního seznamu seřazených a povolených CipherSpecs na webu IBM MQ for z/OS .

Duplicitní názvy CipherSpec v seznamu jsou ignorovány.

V 9.3.0 **OutboundSNI**

Zda je SNI (Server Name Indication) nastaven na název cílového kanálu IBM MQ pro vzdálený systém při inicializaci připojení TLS, nebo na název hostitele; platné hodnoty jsou: CHANNEL nebo HOSTNAME.

Pokud je cílový kanál nakonfigurován s popiskem certifikátu v poli objektu kanálu CERTLABL, musíte nastavit CERTLABL na hodnotu kanálu. Pokud je vytvořeno připojení s nastavením HOSTNAME ke kanálu s nastavením CERTLABL, připojení se nezdaří a ve vzdálených protokolech chyb správce front se zobrazí zpráva AMQ9673 .

Následující příklad ukazuje, jak je uvedena sekce `TransportSecurity` :

```
TransportSecurity:
AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256,
                   ECDHE_RSA_AES_256_GCM_SHA384
AllowTLSV13=TRUE
```

z/OS *Vytvořit datové sady zaváděcího programu a protokolu*

Pomocí dodaného programu CSQJU003 připravte datové sady zaváděcího programu (BSDS) a datové sady protokolu.

Poznámka:

- Tuto úlohu opakujte pro všechny správce front IBM MQ .
- Pokud používáte šifrování datové sady z/OS k ochraně BSDS nebo datových sad aktivního protokolu, musíte tuto volbu nakonfigurovat před přidělením datových sad v tomto kroku.
- Tuto úlohu nemusíte provádět při migraci z předchozí verze.
- Pokud provádíte migraci správce front a přidáváte šifrování datové sady z/OS pro datové sady aktivního protokolu nebo BSDS, musíte datové sady převést.
- Další informace o konfiguraci šifrování datové sady z/OS a převodu existujících datových sad produktu IBM MQ na šifrované naleznete v tématu Důvěrné informace o datech, která jsou v systému IBM MQ for z/OS nečinná, se šifrováním datové sady..

V souboru thlqual.SCSQPROC(CSQ4BSDS) jsou uloženy vzorové řídicí příkazy JCL a AMS (Access Method Services) ke spuštění CSQJU003 pro vytvoření jednoho nebo duálního prostředí protokolování. Přizpůsobte a spusťte tuto úlohu, abyste vytvořili BSDS a protokoly a předformátili protokoly.

Důležité: Měli byste použít nejnovější verzi CSQ4BSDSnebo ručně aktualizovat JCL tak, aby používalo RECORDS (850 60).

Spuštěná procedura úlohy CSQ4MSTRpopsaná v části “Vytvořit procedury pro správce front IBM MQ” na stránce 887odkazuje na BSDS v příkazech formuláře:

```
//BSDS1   DD DSN=++HLQ++.BSDS01,DISP=SHR
//BSDS2   DD DSN=++HLQ++.BSDS02,DISP=SHR
```

Datové sady protokolu jsou odkazovány pomocí BSDS.

Poznámka:

1. V příkazu SYSPRINT DD v kroku LOGDEF musí být zadána hodnota BLKSIZE. Hodnota BLKSIZE musí být 629.
2. Chcete-li pomoci identifikovat datové sady samozavedení a datové sady protokolu z různých správců front, zahrňte název subsystému do kvalifikátoru vysoké úrovně těchto datových sad.
3. Používáte-li skupiny sdílení front, musíte definovat datové sady zaváděcího programu a protokolu s volbou SHAREOPTIONS (2 3).

Informace o plánování samozavedení a datových sadách protokolu a jejich velikosti naleznete v části Plánování v z/OS .

V produktu IBM MQ 8.0vylepšení 8bajtového protokolu RBA zlepšuje dostupnost správce front, jak je popsáno v části Relativní bajtová adresa pro větší protokol. Chcete-li povolit 8bajtový protokol RBA ve správci front před prvním spuštěním správce front, proveďte po vytvoření prostředí protokolování následující kroky.

Poznámka: V 9.3.0 Pro správce front vytvořené v adresáři IBM MQ 9.3.0 nebo novějším je již povolena osmibajtová adresa RBA protokolu, takže následující kroky nejsou nutné.

1. Pomocí produktu **IDCAMS ALTER**přejmenujte formát BSDS verze 1 (vytvořený pomocí programu CSQJU003) na formát ++HLQ++.V1.BSDS01.

   Poznámka: Ujistěte se, že jste přejmenovali komponenty dat a indexu, stejně jako klastr VSAM.
2. Přidělte nové BSDS se stejnými atributy jako ty, které jsou již definovány. Stanou se z nich BSDS ve formátu verze 2, které budou použity správcem front při jeho spuštění.
3. Spusťte obslužný program pro převod BSDS (CSQJUCNV) a převeďte formát BSDS verze 1 na formát BSDS nové verze 2.
4. Po úspěšném dokončení převodu odstraňte formát BSDS verze 1.

Poznámka: Pokud je správce front ve skupině sdílení front, musí být všichni správci front ve skupině sdílení front spuštění následujícím způsobem, než bude možné povolit 8bajtový protokol RBA:

- Je-li správce front na adrese IBM MQ 9.0.0 LTS , musí být spuštěn s volbou **OPMODE**(NEWFUNC,900) nebo **OPMODE**(*NEWFUNC,800*).
- Pokud je správce front v adresáři IBM MQ 9.0.n CD, nebo IBM MQ 9.1.0 LTSnebo novější, musí být spuštěn na této úrovni

Související pojmy

“Definování sad stránek” na stránce 897
Definujte sady stránek pro jednotlivé správce front pomocí jedné z dodaných ukázek.

z/OS *Definování sad stránek*

Definujte sady stránek pro jednotlivé správce front pomocí jedné z dodaných ukázek.

- *Tuto úlohu opakujte pro každého IBM MQ správce front.*

  Pokud k ochraně sad stránek používáte šifrování datové sady z/OS , musíte tuto volbu nakonfigurovat před přidělením datových sad v tomto kroku.
- *Tuto úlohu nemusíte provádět při migraci z předchozí verze.*

  Pokud provádíte migraci správce front a přidáváte šifrování datové sady z/OS pro sady stránek, musíte tyto sady stránek převést.

  Viz část Důvěrnost pro data v klidu IBM MQ for z/OS se šifrováním datové sady. *Další informace o konfiguraci šifrování datové sady z/OS a převodu existujících datových sad IBM MQ na šifrované.*

Definujte samostatné sady stránek pro každého správce front IBM MQ . Příkazy thlqual.SCSQPROC(CSQ4PAGE) a thlqual.SCSQPROC(CSQ4PAGR) obsahují řídicí příkazy JCL a z/OS access method services (AMS) pro definování a formátování sad stránek. Člen CSQ4PAGE používá jednu sadu stránek pro každou třídu zprávy. Člen CSQ4PAGR používá pro hlavní třídy zpráv více sad stránek. JCL spouští dodaný obslužný program CSQUTIL. Zkontrolujte ukázky a upravte je pro požadovaný počet sad stránek a velikosti, které se mají použít. Informace o sadách stránek a způsobu výpočtu vhodných velikostí naleznete v tématu Plánování sad stránek a fondů vyrovnávacích pamětí .

Spuštěná procedura úlohy CSQ4MSTR popsaná v tématu “Vytvořit procedury pro správce front IBM MQ” na stránce 887 odkazuje na sady stránek v příkazu formuláře:

```
//CSQP00nn DD DISP=OLD,DSN=xxxxxxxxxx
```

kde *nn* je číslo sady stránek mezi 00 a 99 a *xxxxxxxxxx* je datová sada, kterou definujete.

Poznámka:

1. Chcete-li použít funkci dynamického rozbalení sady stránek, ujistěte se, že jsou pro každou sadu stránek definovány sekundární oblasti. thlqual.SCSQPROC(CSQ4PAGE) ukazuje, jak to provést.
2. Chcete-li pomoci identifikovat sady stránek z různých správců front, zahrňte název subsystému do kvalifikátoru nejvyšší úrovně datové sady přidružené ke každé sadě stránek.
3. Pokud chcete povolit použití volby FORCE s funkcí FORMAT obslužného programu CSQUTIL, musíte přidat atribut REUSE do příkazu AMS DEFINE CLUSTER.

   Další informace o příkazu REUSE z/OS DEFINE CLUSTER naleznete v části Volitelné parametry .
4. Pokud mají být vaše sady stránek větší než 4 GB, musíte použít funkci SMS (Storage Management System) EXTENDED ADDRESSABILITY.

Související pojmy

"Přidejte položky IBM MQ do tabulek Db2 ." na stránce 930
Používáte-li skupiny sdílení front, spusťte obslužný program CSQ5PQSG a přidejte položky skupiny sdílení front a položky správce front do tabulek IBM MQ ve skupině sdílení dat Db2 .

z/OS *Přizpůsobení modulu systémových parametrů*

Modul systémových parametrů IBM MQ řídí prostředí protokolování, archivace, trasování a připojení, která produkt IBM MQ používá ve své činnosti. Je dodán výchozí modul. Měli byste vytvořit svůj vlastní modul systémových parametrů, protože některé parametry, například názvy datových sad, jsou obvykle specifické pro daný server.

- *Opakujte tuto úlohu pro každého IBM MQ správce front podle potřeby.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze. Podrobnosti viz* Migrace IBM MQ na z/OS.
- *Chcete-li povolit Advanced Message Security for z/OS v existujícím správci front, musíte nastavit parametr SPLCAP pouze na hodnotu YES, jak je popsáno v tématu* "Použití CSQ6SYSP" na stránce 900. *Pokud konfigurujete tohoto správce front poprvé, proveďte celou tuto úlohu.*

Modul systémových parametrů má čtyři makra:

Název makra	Účel
CSQ6SYSP	Určuje parametry připojení a trasování, viz "Použití CSQ6SYSP" na stránce 900 .
CSQ6LOGP	Řídí inicializaci protokolu, viz "Použití CSQ6LOGP" na stránce 909
CSQ6ARVP	Řídí inicializaci archivu, viz "Použití CSQ6ARVP" na stránce 914
CSQ6USGP	Řídí záznam použití, viz "Použití CSQ6USGP" na stránce 921

IBM MQ dodává výchozí modul systémových parametrů CSQZPARM, který se vyvolá automaticky, pokud zadáte příkaz START QMGR (bez parametru PARM) pro spuštění instance IBM MQ. CSQZPARM je v knihovně s oprávněním APF thlqual.SCSQAUTH také dodávané s produktem IBM MQ. Hodnoty těchto parametrů se při spuštění produktu IBM MQzobrazí jako posloupnost zpráv.

Další informace o použití tohoto příkazu viz START QMGR .

Vytvoření vlastního modulu systémových parametrů

Pokud CSQZPARM neobsahuje požadované systémové parametry, můžete vytvořit vlastní modul systémových parametrů pomocí ukázkového JCL uvedeného v souboru thlqual.SCSQPROC(CSQ4ZPRM).

Chcete-li vytvořit vlastní modul systémových parametrů, postupujte takto:

1. Vytvořte pracovní kopii ukázky JCL.

2. Upravte parametry pro každé makro v kopii podle potřeby. Pokud z volání makra odeberete nějaké parametry, výchozí hodnoty se automaticky vyzvednou za běhu.
3. Nahraďte zástupný symbol ++NAME++ názvem, který má zaváděcí modul převzít (může to být CSQZPARM).
4. Pokud váš sestavovací modul není sestavovací modul vysoké úrovně, změňte JCL podle potřeby vašeho sestavovacího modulu.
5. Spusťte skript JCL, který sestaví a propojí upravené verze maker systémových parametrů, aby vytvořil zaváděcí modul. Jedná se o nový modul parametrů systému s názvem, který jste zadali.
6. Vložte zaváděcí modul vytvořený v knihovně autorizovaného uživatele APF.
7. Přidejte uživatelský přístup READ ke knihovně autorizovaného uživatele APF.
8. Zahrňte tuto knihovnu do procedury STEPLIB spuštěné úlohy správce front IBM MQ . Tento název knihovny musí být uveden před knihovnou thlqual.SCSQAUTH v knihovně STEPLIB.
9. Vyvolejte nový modul systémových parametrů při spuštění správce front. Pokud je například nový modul nazván NEWMODS, zadejte příkaz:

```
START QMGR PARM(NEWMODS)
```

10. Zkontrolujte protokol úlohy a ujistěte se, že příkaz byl úspěšně dokončen. V protokolu by měla být položka podobná následující:

```
CSQ9022I CDL1 CSQYASCP 'START QMGR' NORMAL COMPLETION
```

Můžete také zadat název modulu parametrů ve spouštěcím kódu JCL správce front. Další informace naleznete v tématu Použití MQSC ke spuštění a zastavení správce front v systému z/OS.

Poznámka: Pokud se rozhodnete pojmenovat modul CSQZPARM, nemusíte zadávat parametr PARM v příkazu START QMGR.

Doladění modulu systémových parametrů

Produkt IBM MQ také dodává sadu tří zdrojových modulů asembleru, které lze použít k vyladění existujícího modulu systémových parametrů. Tyto moduly jsou v knihovně thlqual.SCSQASMS. Tyto moduly zpravidla používáte v testovacím prostředí ke změně výchozích parametrů v makrech systémových parametrů. Každý zdrojový modul volá jiné makro parametrů systému:

Tento zdrojový modul sestavovacího modulu ...	**Volá toto makro ...**
CSQFSYSP	CSQ6SYSP (parametry připojení a trasování)
CSQJLOGP	CSQ6LOGP (inicializace protokolu)
CSQJARVP	CSQ6ARVP (inicializace archivu)

Tímto způsobem používáte tyto moduly:

1. Vytvořte pracovní kopie každého zdrojového modulu asembleru v knihovně uživatelského asembleru.
2. Upravte kopie přidáním nebo změnou hodnot libovolných parametrů podle potřeby.
3. Sestavte kopie všech upravených modulů, abyste vytvořili moduly objektů v knihovně uživatelských objektů.
4. Upravte tyto moduly objektového kódu s existujícím modulem systémových parametrů tak, aby produkoval zaváděcí modul, který je novým modulem systémových parametrů.
5. Ujistěte se, že nový modul systémových parametrů je členem uživatelem autorizované knihovny.

6. Zahrňte tuto knihovnu do procedury STEPLIB spuštěné úlohy správce front. Tato knihovna musí být před knihovnou thlqual.SCSQAUTH v knihovně STEPLIB.
7. Vyvolejte nový modul systémových parametrů zadáním příkazu START QMGR a zadáním názvu nového modulu v parametru PARM jako dříve.

Ukázkový usermod je poskytován ve členu CSQ4UZPR SCSQPROC, který demonstruje, jak spravovat upravené systémové parametry pod řízením SMP/E.

Změna parametrů systému

V době, kdy je spuštěn správce front, můžete změnit některé parametry systému. Viz příkazy SET SYSTEM, SET LOGa SET ARCHIVE .

Vložte příkazy SET do vstupních datových sad inicializace tak, aby se projevily při každém spuštění správce front.

Související pojmy

“Přizpůsobit parametry inicializátoru kanálu” na stránce 922
Pomocí příkazu ALTER QMGR upravte inicializátor kanálu tak, aby vyhovoval vašim požadavkům.

z/OS *Použití CSQ6SYSP*

Toto téma slouží jako reference pro nastavení systémových parametrů pomocí CSQ6SYSP.

Výchozí parametry pro CSQ6SYSPa zda můžete každý parametr změnit pomocí příkazu SET SYSTEM, jsou uvedeny v části Tabulka 59 na stránce 900. Chcete-li změnit některou z těchto hodnot, prohlédněte si podrobný popis parametrů.

Tabulka 59. Výchozí hodnoty parametrů CSQ6SYSP

Parametr	Popis	Výchozí hodnota	Příkaz SET
V 9.3.0 “[MQ 9.3.0, červenec 2021]ACCTIME ” na stránce 902	Doba v minutách a sekundách mezi každým shromažďováním dat evidence.	-1	✓
“ACELIM” na stránce 902	Velikost fondu úložišť ACE v 1 KB blocích.	0 (bez omezení)	✓
“CLCACHE” na stránce 903	Určuje typ mezipaměti klastru, která má být použita.	STATICKÝ	-
“CMDUSER” na stránce 903	Výchozí ID uživatele pro kontroly zabezpečení příkazu.	CSQOPR	-
“EXCLMSG” na stránce 903	Uvádí seznam zpráv, které mají být vyloučeny z jakéhokoli protokolu. Zprávy v tomto seznamu nejsou odesílány na konzolu z/OS a do protokolu tištěné kopie. V důsledku toho je použití parametru EXCLMSG k vyloučení zpráv z perspektivy CPU efektivnější než použití metod popsaných v tématu “Potlačit informační zprávy” na stránce 926 .	( )	✓
“EXITLIM” na stránce 904	Maximální doba (v sekundách), po kterou mohou být uživatelské procedury správce front spuštěny během každého vyvolání.	30	-

Tabulka 59. Výchozí hodnoty parametrů CSQ6SYSP (pokračování)			
Parametr	**Popis**	**Výchozí hodnota**	**Příkaz SET**
“EXITTCB” na stránce 904	Počet spuštěných úloh serveru, které mají být použity ke spuštění uživatelských procedur správce front.	8	-
“LOGLOAD” na stránce 904	Počet záznamů protokolu zapsaných produktem IBM MQ mezi začátkem jednoho kontrolního bodu a dalším kontrolním bodem.	500 000	✓
“MULCCAPT” na stránce 904	Určuje vlastnost Ceny měřeného využití, která řídí algoritmus pro shromažďování dat používaných MULC (Již Měřeno využití licencí).	Viz popis parametru .	-
“OTMACON” na stránce 905	Parametry připojení OTMA.	Viz popis parametru .	-
“QINDXBLD” na stránce 905	Určuje, zda má restartování správce front čekat na opětné sestavení všech indexů nebo zda má být dokončeno opětné sestavení všech indexů.	WAIT	-
“QMCCSID” na stránce 906	Identifikátor kódované znakové sady pro správce front.	Nula	-
“QSGDATA” na stránce 906	Parametry skupiny sdílení front.	Viz popis parametru .	-
“RESAUDIT” na stránce 907	Parametr auditování RESLEVEL.	YES	-
“ROUTCDE” na stránce 907	Kód směrování zpráv přiřazený ke zprávám, které nebyly vyžádány ze specifické konzoly.	1	-
“SERVICE” na stránce 907	Vyhrazeno pro použití společností IBM.	0	✓
“SMFACCT” na stránce 907	Určuje, zda mají být při spuštění správce front shromažďována data evidence SMF. Všimněte si, že data evidence kanálu třídy 4 jsou shromažďována pouze při spuštění inicializátoru kanálu.	NO	-
SMFSTAT	Určuje, zda mají být při spuštění správce front shromažďovány statistické údaje SMF. Mějte na paměti, že statistická data inicializátoru kanálu třídy 4 jsou shromažďována pouze při spuštění inicializátoru kanálu.	NO	-
SPLCAP	Určuje, zda je v tomto správci front povolena možnost použití zásad zabezpečení fronty. Pro parametr Advanced Message Security for z/OSnastavte tento parametr na hodnotu YES.	NO	-
STATIME	V 9.3.0 Doba, v minutách a sekundách, mezi každým shromažďováním statistik.	30	✓
TRACSTR	Určuje, zda má být trasování spuštěno automaticky.	NO	-

Tabulka 59. Výchozí hodnoty parametrů CSQ6SYSP (pokračování)			
Parametr	**Popis**	**Výchozí hodnota**	**Příkaz SET**
TRACTBL	Velikost trasovací tabulky v blocích o velikosti 4 kB, která má být použita globálním trasovacím prostředkem.	99 (396 kB)	✓
WLMTIME	Doba mezi skenováním indexu fronty pro fronty spravované WLM.	30	-
WLMTIMU	Jednotky (minuty nebo sekundy) pro WLMTIME.	minuty	-

V 9.3.0 **ACCTIME**

Určuje interval v minutách a sekundách mezi následnými shromažďeními dat evidence.

Zadejte číslo, buď `-1`, nebo v rozsahu `0` až `1440` minut ve formátu `'mmmm'`, nebo v rozsahu `0` až `1440` minut a `0` -`59` sekund, ve formátu `'mmmm.ss'`.

Notes:

- Při zadávání pouze intervalu v sekundách musíte před interval zadat hodnotu `0`. Nejmenší možný interval je jedna sekunda: '`0.01`'.
- Zadáte-li hodnotu `0`, budou data evidence shromažďována v globálním intervalu záznamu SMF. Další informace naleznete v tématu Použití zařízení pro správu systému .
- Zadáte-li hodnotu `-1`, která je výchozí, budou data evidence shromažďována v intervalu určeném hodnotou STATIME.

Příklad:

`'0.30'` nastaví interval 30 sekund.
`'5.30'` nastaví interval 5 minut a 30 sekund.
`'30'` nastavuje interval 30 minut.

ACELIM

Určuje maximální velikost fondu úložišť ACE v 1kB blocích. Číslo musí být v rozsahu 0-999999. Výchozí hodnota nula znamená, že nejsou určena žádná omezení nad rámec možností systému.

Hodnotu ACELIM byste měli nastavit pouze pro správce front, u nichž bylo zjištěno nadměrné používání úložiště ECSA. Omezení fondu úložišť ACE je limitováno počtem připojení v systému, a tedy množstvím úložiště ECSA používané správcem front.

Jakmile správce front dosáhne limitu, není možné pro aplikace získat nová připojení. Nedostatek nových připojení způsobí selhání ve zpracování MQCONN a u aplikací koordinovaných prostřednictvím služby RRS bude pravděpodobně docházet k selháním v nějakém rozhraníIBM MQ API.

Položka řízení přístupu (ACE) představuje přibližně 12,5 % z celkové hodnoty ECSA vyžadované pro řídicí bloky připojení, které souvisí s podprocesy. Lze tedy například očekávat, že zadáte-li hodnotu ACELIM=5120 , celkové množství ECSA přidělené správcem front (pro řídicí bloky související s podprocesy) bude přibližně 40960K; , tj. 5120 krát 8.

Pro omezení celkového množství ECSA přiděleného správcem front je pro řídicí bloky související s podprocesy s hodnotou 5120Kvyžadována hodnota ACELIM 640.

Prostřednictvím záznamů SMF 115 subtype 7 zhotovovaných trasováním statistiky CLASS(3) lze monitorovat velikost fondu úložišť 'ACE/PEB, a následně nastavit vhodnou hodnotu ACELIM.

Informaci, jaké celkové množství úložiště ECSA používá správce front pro řídicí bloky, lze získat ze záznamů SMF 115 subtype 7 zapisovaných trasováním statistiky CLASS(2). Celková velikost použité paměti ECSA je součtem polí QSRSPHBGF a QSRSPHBGV.

Další informace o záznamech statistiky SMF 115 viz Interpretace statistiky výkonu produktu IBM MQ.

Poznámka: Nastavení ACELIM by mělo sloužit jako mechanizmus k ochraně obrazu z/OS před špatným chováním správce front, nikoli jako prostředek k řízení připojení aplikací ke správci front.

CLCACHE
Určuje typ mezipaměti klastru, která má být použita.

Mezipaměť klastru je oblast úložiště používaná k ukládání informací souvisejících s klastrem.

Pokud je mezipaměť klastru statická, má pevnou velikost, která je přidělena při spuštění správce front. Pokud se mezipaměť zaplní, je vydána zpráva CSQM060E a požadavek aplikace, který vyžadoval více prostoru, obdrží zprávu MQRC_CLUSTER_RESOURCE_ERROR.

Nastavíte-li parametr CLCACHE na dynamický, může se mezipaměť klastru podle potřeby rozbalit. Nejprve však musíte zajistit, aby všechny nainstalované uživatelské procedury pracovní zátěže klastru fungovaly s dynamickou mezipamětí.

Pokud instalovaná uživatelská procedura pracovní zátěže klastru nemůže fungovat se zprávou dynamické mezipaměti CSQM061E je vydána.

MQXCLWLNje k dispozici pro uživatelské procedury pracovní zátěže klastru pro navigaci v mezipaměti klastru způsobem, který funguje bez ohledu na to, zda jsou použity dynamické nebo statické mezipaměti.

Pro nové správce front nastavte parametr CLCACHE=DYNAMIC, pokud nepoužijete uživatelskou proceduru pracovní zátěže klastru, která nepodporuje dynamickou mezipaměť.

Pro existující správce front, kteří již používají statickou mezipaměť a jsou v klastru, do kterého není přidáno mnoho nových front a správců front, je vhodné pokračovat v používání parametru CLCACHE=STATIC.

Pro existující správce front, kteří již používají statickou mezipaměť a jsou v klastru, do kterého bude přidáno mnoho nových front nebo správců front, začněte používat CLCACHE=DYNAMIC.

STATICKÝ
Je-li mezipaměť klastru statická, její velikost je při spuštění správce front pevná, což je dostačující pro aktuální množství informací o klastru plus prostor pro rozšíření. Velikost nelze zvýšit, pokud je správce front aktivní. Toto nastavení je výchozí.

DYNAMICKÝ
Je-li mezipaměť klastru dynamická, lze počáteční velikost přidělenou při spuštění správce front automaticky zvýšit, je-li to vyžadováno v době, kdy je správce front aktivní.

CMDUSER
Určuje výchozí ID uživatele použité pro kontroly zabezpečení příkazu. Toto ID uživatele musí být definováno pro ESM (například RACF). Zadejte název o délce 1 až 8 alfanumerických znaků. První znak musí být písmeno.

Výchozí hodnota je CSQOPR.

EXCLMSG
Uvádí seznam chybových zpráv, které se mají vyloučit.

Tento seznam je dynamický a je aktualizován pomocí příkazu SET SYSTEM.

Výchozí hodnota je prázdný list ().

Zprávy jsou dodávány bez předpony CSQ a bez přípony kódu akce (I-D-E-A). Chcete-li například vyloučit zprávu CSQX500I, přidejte do tohoto seznamu X500 . Tento seznam může obsahovat maximálně 16 identifikátorů zpráv.

Aby byla zpráva způsobilá k zařazení do seznamu, musí být vydána po normálním spuštění adresních prostorů MSTR nebo CHIN a musí začínat jedním z následujících znaků E, H, I, J, L, M, N, P, R, T, V, W, X, Y, 2, 3, 5, 9.

Identifikátory zpráv, které jsou vydány jako výsledek zpracování příkazů, mohou být přidány do seznamu, ale nebudou vyloučeny. Například identifikátor zprávy je vydán jako výsledek příkazu DISPLAY USAGE PSID (*), avšak tuto zprávu nelze potlačit.

EXITLIM
Určuje dobu (v sekundách) povolenou pro každé vyvolání uživatelských procedur správce front. (Tento parametr nemá žádný vliv na uživatelské procedury kanálu.)

Uveďte hodnotu v rozsahu 5 až 9999.

Výchozí hodnota je 30. Správce front se dotazuje uživatelských procedur, které jsou spuštěny každých 30 sekund. V každé výzvě jsou všechny výzvy, které byly spuštěny déle, než je čas určený parametrem EXITLIM, vynuceně ukončeny.

EXITTCB
Určuje počet spuštěných úloh serveru, které mají být použity ke spuštění uživatelských procedur ve správci front. (Tento parametr nemá žádný vliv na uživatelské procedury kanálu.) Musíte zadat číslo alespoň tak vysoké, jako je maximální počet uživatelských procedur (jiných než uživatelských procedur kanálu), které bude muset správce front spustit, jinak dojde k selhání s nestandardním ukončením 6c6 .

Zadejte hodnotu v rozsahu od 0 do 99. Hodnota nula znamená, že nelze spustit žádné uživatelské procedury.

Výchozí hodnota je 8.

LOGLOAD
Určuje počet záznamů protokolu, které produkt IBM MQ zapisuje mezi začátkem jednoho kontrolního bodu a dalším. Produkt IBM MQ zahájí nový kontrolní bod po zapsání počtu záznamů, které zadáte.

Zadejte hodnotu v rozsahu 200 až 16 000 000.

Výchozí hodnota je 500 000.

Čím vyšší hodnota, tím lepší výkon IBM MQ ; Restart však trvá déle, pokud je parametr nastaven na velkou hodnotu.

Navrhovaná nastavení:

Testovací systém	10 000
Výrobní systém	500 000 V produkčním systému může zadaná výchozí hodnota vést k příliš vysoké frekvenci kontrolních bodů.

Hodnota LOGLOAD určuje frekvenci kontrolních bodů správce front. Příliš velká hodnota znamená, že se do protokolu mezi kontrolními body zapíše velké množství dat, což má za následek delší dobu dopředného zotavení správce front po selhání. Příliš malá hodnota způsobí, že se kontrolní body vyskytnou příliš často během špičkového zatížení, což nepříznivě ovlivní dobu odezvy a využití procesoru.

Pro obslužný program LOGLOAD se doporučuje počáteční hodnota 500 000. Pro rychlost trvalých zpráv o velikosti 1 kB 100 zpráv za sekundu (tj. 100 MQPUT s potvrzením a 100 MQGET s potvrzením) je interval mezi kontrolními body přibližně 5 minut.

Poznámka: To je určeno pouze jako vodítko a optimální hodnota pro tento parametr je závislá na charakteristice jednotlivých systémů.

MULCCAPT
Uvádí algoritmus, který se má použít pro shromažďování dat používaných MULC (Meměřeno Usage License Charging).

STANDARD
MULC je založeno na čase volání MQCONN rozhraní API produktu IBM MQ do času volání MQDISC rozhraní API produktu IBM MQ .

Upřesněno
MULC je založeno na čase od spuštění volání rozhraní API IBM MQ do konce volání rozhraní API IBM MQ .

Výchozí hodnota je STANDARD.

OTMACON
Parametry OTMA. Toto klíčové slovo má pět pozičních parametrů:

OTMACON = (`Group,Member,Druexit,Age,Tpipepfx`)

Skupina
Jedná se o název skupiny XCF, do které náleží tato konkrétní instance produktu IBM MQ .

Může být dlouhý 1 až 8 znaků a musí být zadán velkými písmeny.

Výchozí hodnotou jsou mezery, což znamená, že se produkt IBM MQ nesmí pokoušet o připojení ke skupině XCF.

Člen
Jedná se o název člena této konkrétní instance produktu IBM MQ ve skupině XCF.

Může být dlouhý 1 až 16 znaků a musí být zadán velkými písmeny.

Výchozí hodnota je 4znakový název správce front.

Výjezd z výjezdu
Tato volba určuje název uživatelské procedury rozpoznání místa určení OTMA, kterou má spustit program IMS.

Může mít délku 1 až 8 znaků.

Předvolba je DFSYDRU0.

Tento parametr je volitelný; je povinný, pokud má produkt IBM MQ přijímat zprávy z aplikace IMS , která nebyla spuštěna produktem IBM MQ. Název musí odpovídat uživatelské proceduře rozpoznání místa určení kódované v systému IMS . Další informace viz “Použití uživatelských procedur OTMA v adresáři IMS” na stránce 991.

Věk
Toto představuje dobu v sekundách, po kterou je ID uživatele z produktu IBM MQ považováno za dříve ověřené produktem IMS.

Může být v rozsahu nula až 2 147 483 647.

Výchozí hodnota je 2 147 483 647.

Doporučuje se nastavit tento parametr společně s parametrem `interval` příkazu ALTER SECURITY, aby byla zachována konzistence nastavení mezipaměti zabezpečení v rámci sálového počítače.

Tpipepfx
Toto představuje předponu, která se má použít pro názvy Tpipe.

Skládá se ze tří znaků; první znak je v rozsahu A až Z, následující znaky jsou A až Z nebo 0 až 9. Výchozí nastavení je CSQ.

Používá se pokaždé, když produkt IBM MQ vytvoří Tpipe; zbytek názvu je přiřazen produktem IBM MQ. Nemůžete nastavit úplný název propojení procesů pro žádné propojení procesů vytvořené produktem IBM MQ.

QINDXBLD
Určuje, zda má restartování správce front čekat na opětné sestavení všech indexů front nebo zda má být dokončeno opětné sestavení všech indexů.

WAIT
Restart správce front čeká na dokončení všech sestavení indexů front. To znamená, že během normálního zpracování rozhraní IBM MQ API při vytváření indexu nejsou zpožděny žádné aplikace, protože všechny indexy jsou vytvořeny dříve, než se aplikace mohou připojit ke správci front.

Toto nastavení je výchozí.

NoWait
Správce front může být restartován před dokončením sestavování všech indexů front.

QMCCSID
Určuje výchozí identifikátor kódované znakové sady, který má použít správce front (a tedy distribuované řazení do front).

Uveďte hodnotu v rozsahu nula až 65535. Hodnota musí představovat kódovou stránku EBCDIC uvedenou jako nativní z/OS kódová stránka pro zvolený jazyk v národních jazycích.

Nula, což je výchozí hodnota, znamená použít momentálně nastavený CCSID, nebo, pokud není žádný nastaven, použít CCSID 500. To znamená, že pokud jste explicitně nastavili CCSID na nenulovou hodnotu, nemůžete jej resetovat nastavením QMCCSID na nulu; nyní musíte použít správný nenulový CCSID. Je-li QMCCSID nula, můžete zkontrolovat, který CCSID se skutečně používá, zadáním příkazu DISPLAY QMGR CCSID.

Poznámka: Všichni správci front ve skupině sdílení front by měli používat stejný identifikátor QMCCSID.

QSGDATA
Data skupiny sdílení front. Toto klíčové slovo má pět pozičních parametrů:

QSGDATA = (Qsgname,Dsgname,Db2name,Db2serv ,Db2blob)

QSGNAME
Jedná se o název skupiny sdílení front, do které patří daný správce front.

Platné znaky viz Pravidla pro pojmenování IBM MQ objektů . Název:

- Může být dlouhý 1 až 4 znaky
- Nesmí začínat číslem
- Nesmí končit znakem @.

  Důvodem je, že z implementačních důvodů jsou názvy kratší než čtyři znaky vnitřně doplněny symboly @,

Výchozí hodnotou jsou mezery, které označují, že správce front není členem žádné skupiny sdílení front.

Název_dsgname
Jedná se o název skupiny sdílení dat Db2 , ke které se má správce front připojit.

Může být dlouhý 1 až 8 znaků a musí být zadán velkými písmeny.

Předvolba je mezery, což označuje, že nepoužíváte skupiny sdílení front.

Db2name
Jedná se o název připojení subsystému nebo skupiny Db2 , ke kterému se má správce front připojit.

Může být dlouhý 1 až 4 znaky a musí být zadán velkými písmeny.

Předvolba je mezery, což označuje, že nepoužíváte skupiny sdílení front.

Poznámka: Subsystém Db2 (nebo příloha skupiny) musí být ve skupině sdílení dat Db2 určené v souboru Dsgnamea všichni správci front musí určovat stejnou skupinu sdílení dat Db2 .

Db2serv
Jedná se o počet úloh serveru, které se používají pro přístup k souboru Db2.

Může být v rozsahu 4 až 10.

Výchozí hodnota je 4.

Db2blob
Jedná se o počet úloh Db2 používaných pro přístup k binárním velkým objektům (BLOB).

Může být v rozsahu 4 až 10.

Výchozí hodnota je 4.

Pokud zadáte jeden z parametrů názvu (tj. **Qsgname**, **Dsgname**nebo **Db2name**), musíte zadat hodnoty pro ostatní názvy, jinak IBM MQ selže.

RESAUDIT
Uvádí, zda se záznamy auditu RACF zapisují pro kontroly zabezpečení RESLEVEL prováděné během zpracování připojení.

Zadejte jednu z následujících možností:

NO
Auditování RESLEVEL se neprovádí.

YES
Provádí se auditování RESLEVEL.

Výchozí hodnota je ANO.

ROUTCDE
Určuje výchozí kód směrování zpráv z/OS přiřazený ke zprávám, které nejsou odesílány v přímé reakci na příkaz MQSC.

Zadejte jednu z následujících možností:

1. Hodnota v rozsahu 1 až 16 včetně.
2. Seznam hodnot oddělených čárkou a uzavřených v závorkách. Každá hodnota musí být v rozsahu 1 až 16 včetně.

Výchozí hodnota je 1.

Další informace o kódech směrování systému z/OS naleznete v tématu *Kódy směrování* v části *Popis zprávy* na jednom z nosičů příruček *z/OS Systémové zprávy MVS* .

SERVICE
Toto pole je vyhrazeno pro použití produktem IBM.

SMFACCT
Určuje, zda produkt IBM MQ odesílá data evidence do prostředí SMF automaticky při spuštění správce front.

Zadejte jednu z následujících možností:

NO
Nespouštějte automatické shromažďování dat evidence.

YES
Automaticky spustit shromažďování dat evidence pro výchozí třídu 1.

celá čísla
V 9.3.0 Seznam tříd, pro které jsou data evidence automaticky shromažďována v rozsahu 1 až 4.

V 9.3.0 * Automaticky spustit účtování SMF pro třídy 1, 2 a 3.

Výchozí hodnota je NO.

SMFSTAT
Určuje, zda má být při spuštění správce front automaticky shromažďována statistika SMF.

Zadejte jednu z následujících možností:

NO
Nespouštějte shromažďování statistik automaticky.

YES
Automaticky spustit shromažďování statistik pro výchozí třídu 1.

celá čísla

V 9.3.0 Seznam tříd, pro které jsou statistiky automaticky shromažďovány v rozsahu 1 až 5.

Chcete-li shromáždit statistiku třídy 2 nebo 3, musí být uvedena také třída 1.

V 9.3.0 * Automaticky spustit statistiku SMF pro třídy 1, 2 a 3.

Výchozí hodnota je NO.

SPLCAP

Schopnost zásad zabezpečení umožňuje vyšší úroveň zabezpečení zpráv prostřednictvím zásad, které řídí, zda jsou zprávy podepsány nebo šifrovány při zápisu a čtení z front.

Zpracování zásad zabezpečení je pro tohoto správce front konfigurováno nastavením parametru SPLCAP na jednu z následujících hodnot:

NO

Schopnost implementovat zásady zabezpečení zpráv pro fronty není během inicializace správce front povolena.

YES

Během inicializace správce front jsou povoleny možnosti zabezpečení zpráv.

Správce front kontroluje, zda je atribut AMSPROD nastaven na hodnotu AMS, ADVANCED nebo ADVANCEDVUE. V takovém případě je licencován pro AMS. Jinak se nespustí.

Správce front také kontroluje, zda je zavedena nezbytná konfigurace AMS . Pokud není, správce front se nespustí.

Je-li správce front licencován pro produkt AMSa je-li zavedena nezbytná konfigurace, spustí se správce front s povolenými funkcemi zabezpečení zpráv během inicializace správce front a spustí se adresní prostor AMSM.

Výchozí hodnota je NO.

STATIME

V 9.3.0 Hodnota IBM MQ for z/OS 9.3.0určuje čas v minutách a sekundách mezi následnými shromažďeními statistických dat. Není-li hodnota ACCTIME nastavena nebo je-li hodnota `-1`, určuje také čas mezi následnými shromažďeními dat evidence.

Zadejte číslo v rozsahu `0` až 1440 minut ve formátu `'mmmm'` nebo v rozsahu `0` až 1440 minut a `0` -59 sekund ve formátu `'mmmm.ss'`. Výchozí hodnota je 30 minut.

Notes:

- Při zadávání pouze intervalu v sekundách musíte před interval zadat hodnotu `0`. Nejmenší možný interval je jedna sekunda: `'0.01'`.
- V 9.3.0 Pokud v produktu IBM MQ for z/OS 9.3.0zadáte hodnotu `0`, budou statistická data shromažďována ve všesměrovém vysílání shromažďování dat SMF. Pokud ACCTIME není uvedeno nebo je `-1`, pak se data evidence shromažďují také ve všesměrovém vysílání shromažďování dat SMF. Další informace naleznete v tématu Použití zařízení pro správu systému .
- Zadáte-li hodnotu `-1`, která je výchozí, budou data evidence shromažďována v intervalu určeném hodnotou STATIME.

TRACSTR

Určuje, zda se má globální trasování spouštět automaticky.

Zadejte jednu z následujících možností:

NO

Nespouštět globální trasování automaticky.

YES

Automaticky spustit globální trasování pro výchozí třídu, třídu 1.

celá čísla
Seznam tříd, pro které se má automaticky spustit globální trasování v rozsahu 1 až 4.

*****
Spustit globální trasování automaticky pro všechny třídy.

Výchozí hodnota je NO, pokud v makru nezadáte klíčové slovo.

Poznámka: Dodaný předvolený zaváděcí modul parametrů systému (CSQZPARM) má hodnotu TRACSTR=YES (nastavenou v modulu assembleru CSQFSYSP). Pokud nechcete spustit trasování automaticky, buď vytvořte vlastní modul systémových parametrů, nebo zadejte příkaz STOP TRACE po spuštění správce front.

Podrobnosti o příkazu STOP TRACE viz STOP TRACE.

TRACTBL
Určuje výchozí velikost trasovací tabulky (v blocích o velikosti 4 kB), do které globální trasovací prostředek ukládá IBM MQ trasovací záznamy.

Uveďte hodnotu v rozsahu 1 až 999.

Výchozí hodnota je 99. Jedná se o ekvivalent 396 kB.

Poznámka: Úložiště pro trasovací tabulku je přiděleno v ECSA. Proto musíte tuto hodnotu vybrat opatrně.

WLMTIME
Určuje dobu (v minutách nebo sekundách v závislosti na hodnotě WLMTIMU) mezi jednotlivými skenováním indexů pro fronty spravované WLM.

Uveďte hodnotu v rozsahu 1 až 9999.

Výchozí hodnota je 30.

WLMTIMU
Jednotky času použité s parametrem WLMTIME.

Zadejte jednu z následujících možností:

minuty
Hodnota WLMTIME představuje počet minut.

s
Hodnota WLMTIME představuje počet sekund.

Výchozí hodnota je MINS.

Související odkazy
“Použití CSQ6LOGP” na stránce 909
Toto téma slouží jako reference pro určení voleb protokolování pomocí CSQ6LOGP.

“Použití CSQ6ARVP” na stránce 914
Toto téma slouží jako reference pro určení prostředí archivace pomocí CSQ6ARVP .

z/OS *Použití CSQ6LOGP*
Toto téma slouží jako reference pro určení voleb protokolování pomocí CSQ6LOGP.

K vytvoření voleb protokolování použijte CSQ6LOGP .

Výchozí parametry pro CSQ6LOGPa to, zda můžete jednotlivé parametry změnit pomocí příkazu SET LOG , jsou uvedeny v části Výchozí hodnoty parametrů CSQ6LOGP. Pokud potřebujete změnit některou z těchto hodnot, podívejte se na podrobný popis parametrů.

Tabulka 60. Výchozí hodnoty parametrů CSQ6LOGP			
Parametr	**Popis**	**Výchozí hodnota**	**Příkaz SET**
COMPLOG	Řídí, zda je povolena komprese protokolu.	ŽÁDNÉ	X
DEALLCT	Doba, po kterou zůstane archivní pásková jednotka nevyužita, než bude dealokována.	zero	X
INBUFF	Velikost vstupního úložiště vyrovnávací paměti pro datové sady aktivního a archivního protokolu.	60 kB	-
MAXARCH	Maximální počet svazků protokolu archivace, které lze zaznamenat.	500	X
MAXCNOFF	Maximální počet úloh odlehčování CSQJOFF7 , které lze spustit paralelně.	31	-
MAXRTU	Maximální počet vyhrazených páskových jednotek přidělených k souběžnému čtení páskových nosičů protokolu archivu.	2	X
OFFLOAD	Archivace je zapnuta nebo vypnuta.	ANO (zapnuto)	-
OUTBUFF	Velikost úložiště výstupní vyrovnávací paměti pro datové sady aktivního a archivního protokolu.	4 000 KB	-
TWOACTV	Jednoduché nebo duální aktivní protokolování.	ANO (duální)	-
TWOARCH	Jednoduché nebo duální protokolování archivace.	ANO (duální)	-
TWOBSDS	Jednoduché nebo duální BSDS.	ANO (duální BSDS)	-
WRTHRSH	Počet výstupních vyrovnávacích pamětí, které mají být vyplněny před jejich zápisem do datových sad aktivního protokolu.	20	X
ZHYWRITE	Uvádí, zda je povolena funkce zápisu zHyper.	NO	X

COMPLOG
Určuje, zda je povolena komprese protokolu.

Zadejte jednu z následujících možností:

ŽÁDNÉ
Komprese protokolu není povolena.

RLE
Komprese protokolu je povolena s použitím kódování délky běhu.

ANY
Správce front vybere algoritmus komprese, který poskytuje nejvyšší stupeň komprese záznamu protokolu. Výsledkem této volby je komprese RLE.

Výchozí hodnota je NONE.

Další podrobnosti o kompresi protokolu viz Komprese protokolu.

DEALLCT
Uvádí dobu v minutách, po kterou může pásková jednotka pro čtení archivu zůstat nevyužita, než bude dealokována.

Zadejte jednu z následujících možností:

- Čas, v minutách, v rozsahu nula až 1440

- NOLIMIT

Uvedení 1440 nebo NOLIMIT znamená, že pásková jednotka není nikdy dealokována.

Výchozí hodnota je nula.

Když se data protokolu archivace čtou z pásky, doporučuje se nastavit tuto hodnotu na dostatečně vysokou, abyste umožnili produktu IBM MQ optimalizovat zpracování pásek pro více aplikací pro čtení.

INBUFF
Určuje velikost vstupní vyrovnávací paměti v kilobajtech pro čtení aktivního a archivního protokolu během obnovy. Použijte desetinné číslo v rozsahu 28 až 60. Zadaná hodnota je zaokrouhlena na násobek 4.

Výchozí hodnota je 60 kB.

Navrhovaná nastavení:

Testovací systém	28 kB
Výrobní systém	60 kB Chcete-li dosáhnout nejlepšího výkonu čtení protokolu, nastavte tuto hodnotu na maximum.

MAXARCH
Uvádí maximální počet svazků protokolu archivace, které lze zaznamenat v BSDS. Po překročení tohoto počtu začne záznam znovu na začátku BSDS.

Použijte desetinné číslo v rozsahu 10 až 1000.

Výchozí hodnota je 500.

Navrhovaná nastavení:

Testovací systém	500 (výchozí)
Výrobní systém	1 000 Nastavte tuto hodnotu na maximum, aby služba BSDS mohla zaznamenávat co nejvíce protokolů.

Informace o protokolech a BSDS naleznete v tématu Správa IBM MQ prostředků.

MAXCNOFF
Určuje počet úloh odlehčování CSQJOFF7 , které lze spouštět paralelně.

To umožňuje vyladit správce front nebo správce front tak, aby nepoužívali všechny dostupné páskové jednotky.

Místo toho správce front čeká na dokončení úlohy odlehčování CSQJOFF7 , než se pokusí přidělit nové datové sady archivu.

Pokud správce front archivuje na pásku, nastavte tento parametr tak, aby se počet souběžných požadavků na pásku nerovnal nebo nepřekročil počet dostupných páskových jednotek, jinak by se systém mohl zablokovat.

Všimněte si, že pokud je duální archivace používána, každá úloha odlehčování provede oba archivy, takže parametr musí být nastaven odpovídajícím způsobem. Pokud například správce front provádí duální archivaci na pásku, hodnota MAXCNOFF=2 umožní, aby byly souběžně archivovány až dva aktivní protokoly na čtyři pásky.

Pokud páskové jednotky sdílí několik správců front, měli byste nastavit parametr MAXCNOFF pro každého správce front odpovídajícím způsobem.

Výchozí hodnota je 31.

Uveďte hodnotu v rozsahu 1 až 31.

MAXRTU
Uvádí maximální počet vyhrazených páskových jednotek, které lze přidělit k souběžnému čtení páskových nosičů protokolu archivace.

Tento parametr a parametr DEALLCT umožňují produktu IBM MQ optimalizovat čtení protokolu archivace z páskových zařízení.

Uveďte hodnotu v rozsahu 1 až 99.

Výchozí nastavení je 2.

Doporučuje se, abyste nastavili hodnotu alespoň o jednu menší, než je počet páskových jednotek, které jsou k dispozici pro produkt IBM MQ. Pokud tak učiníte jinak, proces odlehčování může být zpožděn, což může ovlivnit výkon vašeho systému. Chcete-li dosáhnout maximální propustnosti během zpracování protokolu archivace, zadejte pro tuto volbu nejvyšší možnou hodnotu, přičemž si pamatujte, že pro zpracování odlehčování potřebujete alespoň jednu páskovou jednotku.

OFFLOAD
Určuje, zda je archivace zapnuta nebo vypnuta.

Zadejte jednu z následujících možností:

YES
Archivace je zapnuté

NO
Archivace je vypnuta

Výchozí hodnota je ANO.

Upozornění: Nevypínejte archivaci, pokud nepracujete v testovacím prostředí. Pokud ji vypnete, nemůžete zaručit, že data budou obnovena v případě selhání systému nebo transakce.

OUTBUFF
Uvádí celkovou velikost, v kilobajtech, úložiště, které má produkt IBM MQ použít pro výstupní vyrovnávací paměti pro zápis aktivních a archivních datových sad protokolu. Každá výstupní vyrovnávací paměť má velikost 4 kB.

Parametr musí být v rozsahu 128 až 4000. Zadaná hodnota je zaokrouhlena na násobek 4. Hodnoty mezi 40 a 128 budou přijaty z důvodů kompatibility a budou považovány za hodnotu 128.

Výchozí hodnota je 4000 kB.

Navrhovaná nastavení:

Testovací systém	400 kB
Výrobní systém	4 000 KB Nastavte tuto hodnotu na maximum, abyste se vyvarovali spuštění výstupních vyrovnávacích pamětí protokolu.

TWOACTV
Určuje jednoduché nebo duální aktivní protokolování.

Zadejte jednu z následujících možností:

NO
Jednotlivé aktivní protokoly

YES
Duální aktivní protokoly

Výchozí hodnota je ANO.

Další informace o použití jednoduchého a duálního protokolování naleznete v tématu Správa IBM MQ prostředků.

TWOARCH
Určuje počet archivních protokolů, které produkt IBM MQ vytvoří při odlehčení aktivního protokolu.

Zadejte jednu z následujících možností:

NO
Jednotlivé archivní protokoly

YES
Duální archivní protokoly

Výchozí hodnota je ANO.

Navrhovaná nastavení:

Testovací systém	NO
Výrobní systém	YES (výchozí)

Další informace o použití jednoduchého a duálního protokolování naleznete v tématu Správa IBM MQ prostředků.

TWOBSDS
Určuje počet datových sad samozavedení.

Zadejte jednu z následujících možností:

NO
Jeden BSDS

YES
Duální BSDS

Výchozí hodnota je ANO.

Další informace o použití jednoduchého a duálního protokolování naleznete v tématu Správa IBM MQ prostředků.

WRTHRSH
Určuje počet výstupních vyrovnávacích pamětí o velikosti 4 kB, které mají být zaplněny před jejich zápisem do datových sad aktivního protokolu.

Čím větší je počet vyrovnávacích pamětí, tím méně často dochází k zápisu, což zlepšuje výkon produktu IBM MQ. Vyrovnávací paměti mohou být zapsány před dosažením tohoto počtu, dojde-li k významným událostem, například k bodu potvrzení.

Zadejte počet vyrovnávacích pamětí v rozsahu 1 až 256.

Výchozí hodnota je 20.

ZHYWRITE
Uvádí, zda jsou zápisy do aktivních protokolů prováděny s povolenou technologií zHyperWrite.

Další informace o povolení aktivních protokolů s technologií zHyperWrite viz Použití technologie zHyperWrite s aktivními protokoly IBM MQ.

Hodnota může být následující:

NO
zHyperWrite není povolena.

YES
zHyperWrite je povolena.

Související odkazy
“Použití CSQ6SYSP” na stránce 900
Toto téma slouží jako reference pro nastavení systémových parametrů pomocí CSQ6SYSP.

“Použití CSQ6ARVP” na stránce 914
Toto téma slouží jako reference pro určení prostředí archivace pomocí CSQ6ARVP .

z/OS *Použití CSQ6ARVP*

Toto téma slouží jako reference pro určení prostředí archivace pomocí CSQ6ARVP .

K vytvoření svého archivačního prostředí použijte CSQ6ARVP .

Výchozí parametry pro CSQ6ARVPa to, zda lze jednotlivé parametry změnit pomocí příkazu SET ARCHIVE, jsou uvedeny v části Tabulka 61 na stránce 914. Pokud potřebujete změnit některou z těchto hodnot, podívejte se na podrobný popis parametrů. Další informace o plánování úložiště naleznete v tématu Plánování požadavků na úložiště a výkon v produktu z/OS .

Tabulka 61. Výchozí hodnoty parametrů CSQ6ARVP

Parametr	Popis	Výchozí hodnota	Příkaz SET
ALCUNIT	Jednotky, ve kterých se provádí přidělení primárního a sekundárního prostoru.	BLK (bloky)	X
ARCPFX1	Předpona pro první název datové sady protokolu archivace.	CSQARC1	X
ARCPFX2	Předpona pro druhý název datové sady protokolu archivace.	CSQARC2	X
ARCRETN	Doba uchování datové sady protokolu archivace ve dnech.	9999	X
ARCWRTC	Seznam kódů směrování pro zprávy operátorovi o datových sadách protokolu archivace.	1,3,4	X
ARCWTOR	Zda odeslat zprávu operátorovi a počkat na odpověď, než se pokusíte připojit datovou sadu protokolu archivace.	YES	X
BlkSize	Velikost bloku datové sady protokolu archivace.	28 672	X
katalog	Zda jsou datové sady protokolu archivace katalogizovány v ICF.	NO	X
Kompaktní	Zda mají být datové sady protokolu archivace optimalizovány.	NO	X
PRIQTY	Přidělení primárního prostoru pro datové sady DASD.	25 715	X
PROTECT	Zda jsou datové sady protokolu archivace chráněny profily ESM při vytvoření datových sad.	NO	X
QUIESCE	Maximální doba v sekundách, která je povolena pro uvedení do klidového stavu, když je zadán parametr ARCHIVE LOG s parametrem MODE (QUIESCE).	5	X
SECQTY	Přidělení sekundárního prostoru pro datové sady DASD. Informace o jednotkách, které se mají použít, naleznete v parametru ALCUNIT.	540	X
TSTAMP	Zda by měl název datové sady archivu obsahovat časové razítko.	NO	X
UNIT	Typ zařízení nebo název jednotky, na kterém je uložena první kopie datových sad protokolu archivace.	Páska	X

Tabulka 61. Výchozí hodnoty parametrů CSQ6ARVP (pokračování)			
Parametr	**Popis**	**Výchozí hodnota**	**Příkaz SET**
UNIT2	Typ zařízení nebo název jednotky, na kterém je uložena druhá kopie datových sad protokolu archivace.	Prázdný	X

ALCUNIT
Uvádí jednotku, ve které jsou prováděny alokace primárního a sekundárního prostoru.

Zadejte jednu z následujících možností:

CYL
Tlakové láhve

TRK
Stopy

BLK
Bloky

Doporučuje se používat aplikaci BLK, protože je nezávislá na typu zařízení.

Výchozí nastavení je BLK.

Pokud je pravděpodobné, že bude na archivních svazcích DASD fragmentován volný prostor, doporučuje se uvést menší primární oblast a povolit expanzi do sekundárních oblastí. Další informace o přidělení prostoru pro aktivní protokoly naleznete v tématu Plánování archivního úložiště protokolů.

ARCPFX1
Určuje předponu pro název první datové sady protokolu archivace.

Viz parametr TSTAMP, kde naleznete popis toho, jak jsou datové sady pojmenovány, a omezení délky ARCPFX1.

Tento parametr nelze ponechat prázdný.

Výchozí hodnota je CSQARC1.

Možná budete muset autorizovat ID uživatele přidružené k adresnímu prostoru správce front IBM MQ , abyste vytvořili archivní protokoly s touto předponou.

ARCPFX2
Určuje předponu pro název druhé datové sady protokolu archivace.

Viz parametr TSTAMP, kde naleznete popis toho, jak jsou datové sady pojmenovány, a omezení délky ARCPFX2.

Tento parametr nemůže být prázdný, i když je parametr TWOARCH uveden jako NO.

Výchozí nastavení je CSQARC2.

Možná budete muset autorizovat ID uživatele přidružené k adresnímu prostoru správce front IBM MQ , abyste vytvořili archivní protokoly s touto předponou.

ARCRETN
Určuje dobu uchování ve dnech, která má být použita při vytvoření datové sady protokolu archivace.

Parametr musí být v rozsahu od 0 do 9999.

Výchozí hodnota je 9999.

Navrhovaná nastavení:

Testovací systém	3 V testovacím systému nejsou protokoly archivace pravděpodobně vyžadovány po dlouhou dobu.
Výrobní systém	9 999 (výchozí) Nastavte tuto hodnotu na vysokou, chcete-li efektivně vypnout automatické odstranění archivního protokolu.

Další informace o vyřazení datových sad protokolu archivu naleznete v tématu Vyřazení datových sad protokolu archivu.

ARCWRTC
Určuje seznam kódů směrování systému z/OS pro zprávy o datových sadách protokolu archivace pro operátora. Toto pole je ignorováno, pokud je parametr ARCWTOR nastaven na hodnotu NO.

Uveďte až 14 kódů směrování, každý s hodnotou v rozsahu 1 až 16. Musíte zadat alespoň jeden kód. Oddělte kódy v seznamu čárkami, ne mezerami.

Předvolba je seznam hodnot: 1,3,4.

Další informace o kódech směrování systému z/OS naleznete v tématu *Kódy směrování* v části *Popis zprávy* na jednom z nosičů příruček *z/OS Systémové zprávy MVS* .

ARCWTOR
Určuje, zda má být odeslána zpráva operátorovi a přijata odezva před pokusem o připojení datové sady protokolu archivace.

Ostatní uživatelé produktu IBM MQ by mohli být nuceni počkat, než bude datová sada připojena, pokud však produkt IBM MQ čeká na odezvu na zprávu, nemá to na ně vliv.

Zadejte jednu z následujících možností:

YES
Zařízení potřebuje dlouhou dobu k připojení datových sad protokolu archivu. Například pásková jednotka.

NO
Zařízení nemá dlouhé prodlevy. Například DASD.

Výchozí hodnota je ANO.

Navrhovaná nastavení:

Testovací systém	NO
Výrobní systém	YES (výchozí) To závisí na provozních procedurách. Pokud jsou použity páskové roboty, NO může být vhodnější.

BLKSIZE
Určuje velikost bloku datové sady protokolu archivace. Velikost bloku, kterou uvedete, musí být kompatibilní s typem zařízení, který uvedete v parametru UNIT.

Parametr musí být v rozsahu 4 097 až 28 672. Zadaná hodnota je zaokrouhlena na násobek 4 096.

Výchozí hodnota je 28 672.

Tento parametr je přepsán velikostí bloku datové třídy SMS (storage management subsystem), je-li uveden.

Pokud je datová sada protokolu archivace zapsána na DASD, doporučuje se zvolit maximální velikost bloku, která umožňuje dva bloky pro každou stopu. Například pro zařízení 3390 byste měli použít velikost bloku 24 576.

Pokud je datová sada protokolu archivace zapsána na pásku, uvedení největší možné velikosti bloku zvýší rychlost čtení protokolu archivace. Měli byste použít velikost bloku 28 672.

Navrhovaná nastavení:

Testovací systém	Použijte doporučení velikosti bloku v závislosti na médiu použitém pro protokoly archivace. To znamená pro disk 24 576 a pásku 28 672.
Výrobní systém	Použijte doporučení velikosti bloku v závislosti na médiu použitém pro protokoly archivace. To znamená pro disk 24 576 a pásku 28 672.

CATALOG

Uvádí, zda jsou datové sady protokolu archivace katalogovány v primárním katalogu ICF (integrated catalog facility).

Zadejte jednu z následujících možností:

NO
Datové sady protokolu archivace nejsou katalogizovány

YES
Datové sady protokolu archivace jsou katalogizovány

Výchozí hodnota je NO.

Všechny datové sady protokolu archivu přidělené na serveru DASD musí být katalogizovány. Pokud archivujete na DASD s parametrem CATALOG nastaveným na NO, zobrazí se při každém přidělení datové sady protokolu archivace zpráva CSQJ072E a katalogy datové sady IBM MQ .

Navrhovaná nastavení:

Testovací systém	YES
Výrobní systém	ANO, když jsou archivy přiděleny na DASD

COMPACT

Uvádí, zda data zapisovaná do protokolů archivu mají být optimalizována. Tato možnost se používá u zařízení 3480 nebo 3490 s funkcí IDRC (Improved Data Recording Capability). Pokud je tato funkce zapnuta, zapisuje hardware v páskové řídicí jednotce data s daleko vyšší hustotou, než je obvyklé, což umožňuje na každém nosiči uložit více dat. Uveďte NO, pokud nepoužíváte zařízení 3480 s funkcí IDRC nebo základním modelem 3490, s výjimkou 3490E. Chcete-li data komprimovat, zadejte hodnotu YES.

Zadejte jednu z následujících možností:

NO
Neoptimalizovat datové sady

YES
Optimalizovat datové sady

Výchozí hodnota je NO.

Uvedení ANO nepříznivě ovlivňuje výkon. Mějte také na paměti, že data komprimovaná na pásku lze číst pouze pomocí zařízení, které podporuje funkci IDRC. To může být problém, pokud budete muset odeslat archivní pásky na jiný server pro vzdálenou obnovu.

Navrhovaná nastavení:

Testovací systém	Nelze použít

Výrobní systém	NO (výchozí) Týká se pouze komprese IDR 3480 a 3490. Nastavení této volby na hodnotu YES může snížit výkon čtení archivního protokolu během obnovy a restartu; nemá však vliv na zápis na pásku.

PRIQTY

Určuje přidělení primárního prostoru pro datové sady DASD v ALCUNIT.

Hodnota musí být větší než nula.

Výchozí hodnota je 25 715.

Tato hodnota musí být dostatečná pro kopii datové sady protokolu nebo odpovídajícího BSDS, podle toho, která hodnota je větší. Chcete-li určit potřebnou hodnotu, postupujte takto:

1. Určete počet přidělených záznamů aktivního protokolu (c), jak je vysvětleno v části "Vytvořit datové sady zaváděcího programu a protokolu" na stránce 896.
2. Určete počet 4096 bajtových bloků v každém bloku protokolu archivace:

   ```
   d = BLKSIZE / 4096
   ```

   kde BLKSIZE je zaokrouhlená hodnota.
3. Pokud ALCUNIT = BLK:

   ```
   PRIQTY = INT(c / d) + 1
   ```

   kde INT znamená zaokrouhlení dolů na celé číslo.

   Pokud ALCUNIT = TRK:

   ```
   PRIQTY = INT(c / (d * INT(e/BLKSIZE))) + 1
   ```

   kde e je počet bajtů pro každou stopu (56664 pro 3390 zařízení) a INT znamená zaokrouhlení dolů na celé číslo.

   Pokud ALCUNIT = CYL:

   ```
   PRIQTY = INT(c / (d * INT(e/BLKSIZE) * f)) + 1
   ```

   kde f je počet stop pro každý válec (15 pro zařízení 3390) a INT znamená zaokrouhlení dolů na celé číslo.

Chcete-li získat informace o tom, jak velké jsou datové sady protokolů a archivů, prohlédněte si "Vytvořit datové sady zaváděcího programu a protokolu" na stránce 896 a "Definování sad stránek" na stránce 897.

Navrhovaná nastavení:

Testovací systém 1 680

Postačující pro uchování celého aktivního protokolu, tj.:

```
10  080 / 6 = 1  680 blocks
```

Výrobní systém Nelze použít při archivaci na pásku.

Pokud je pravděpodobné, že bude na archivních svazcích DASD fragmentován volný prostor, doporučuje se uvést menší primární oblast a povolit expanzi do sekundárních oblastí. Další informace o přidělení prostoru pro aktivní protokoly naleznete v tématu Plánování archivního úložiště protokolů.

PROTECT
Uvádí, zda mají být datové sady protokolu archivace chráněny diskrétními profily ESM (externího správce zabezpečení) při vytváření datových sad.

Zadejte jednu z následujících možností:

NO
Profily nejsou vytvořeny.

YES
Diskrétní profily datové sady jsou vytvořeny při odlehčování protokolů. Pokud zadáte hodnotu YES:

- Ochrana ESM musí být aktivní pro IBM MQ.
- ID uživatele přidružené k adresnímu prostoru správce front IBM MQ musí mít oprávnění k vytváření těchto profilů.
- Třída TAPEVOL musí být aktivní, pokud archivujete na pásku.

Jinak se odlehčování nezdaří.

Výchozí hodnota je NO.

QUIESCE
Určuje maximální dobu v sekundách povolenou pro uvedení do klidového stavu při zadání příkazu ARCHIVE LOG se zadaným parametrem MODE (QUIESCE).

Parametr musí být v rozsahu 1 až 999.

Výchozí nastavení je 5.

SECQTY
Určuje přidělení sekundárního prostoru pro datové sady DASD v ALCUNIT. Sekundární oblast lze přidělit až 15krát; další informace o ALCUNIT naleznete v příručce IBM z/OS Management Facility Programming Guide .

Parametr musí být větší než nula.

Výchozí hodnota je 540.

TSTAMP
Uvádí, zda název datové sady protokolu archivace obsahuje časovou značku.

Zadejte jednu z následujících možností:

NO
Názvy neobsahují časové razítko. Datové sady protokolu archivu jsou pojmenovány:

```
arcpfxi.A nnnnnnn
```

Kde *arcpfxi* je předpona názvu datové sady uvedená ARCPFX1 nebo ARCPFX2. *arcpfxi* může mít až 35 znaků.

YES
Názvy zahrnují časové razítko. Datové sady protokolu archivu jsou pojmenovány:

```
arcpfxi.cyyddd.T hhmmsst.A nnnnnnn
```

kde *c* je 'D' pro roky do roku 1999 včetně nebo 'E' pro rok 2000 a novější a *arcpfxi* je předpona názvu datové sady určená ARCPFX1 nebo ARCPFX2. *arcpfxi* může mít až 19 znaků.

EXT
Názvy zahrnují časové razítko. Datové sady protokolu archivu jsou pojmenovány:

```
arcpfxi.D yyyyddd.T hhmmsst.A nnnnnnn
```

Kde *arcpfxi* je předpona názvu datové sady uvedená ARCPFX1 nebo ARCPFX2. *arcpfxi* může mít až 17 znaků.

Výchozí hodnota je NO.

UNIT
Uvádí typ zařízení nebo název jednotky zařízení, které se používá k uložení první kopie datové sady protokolu archivace.

Uveďte typ zařízení nebo název jednotky od 1 do 8 alfanumerických znaků. První znak musí být písmeno.

Tento parametr nemůže být prázdný.

Předvolba je TAPE.

Pokud archivujete na DASD, můžete uvést generický typ zařízení s omezeným rozsahem svazků, například UNIT=3390.

Pokud archivujete na DASD, ujistěte se, že:

- Alokace primárního prostoru je dostatečně velká, aby obsahovala všechna data z datových sad aktivního protokolu.
- Volba katalogu datové sady protokolu archivace (CATALOG) je nastavena na hodnotu YES.
- Použili jste správnou hodnotu pro hodnotu BLKSIZE.

Pokud archivujete na TAPE, může produkt IBM MQ rozšířit na maximálně 20 nosičů.

Navrhovaná nastavení:

Testovací systém	DASD
Výrobní systém	Páska

Další informace o výběru umístění protokolů archivace naleznete v tématu Plánování archivního úložiště protokolů.

UNIT2
Uvádí typ zařízení nebo název jednotky zařízení, které se používá k uložení druhé kopie datových sad protokolu archivace.

Uveďte typ zařízení nebo název jednotky od 1 do 8 alfanumerických znaků. První znak musí být písmeno. Je-li tento parametr prázdný, použije se hodnota nastavená pro parametr UNIT.

Výchozí hodnota je prázdná.

Související odkazy
“Použití CSQ6SYSP” na stránce 900
Toto téma slouží jako reference pro nastavení systémových parametrů pomocí CSQ6SYSP.

“Použití CSQ6LOGP” na stránce 909
Toto téma slouží jako reference pro určení voleb protokolování pomocí CSQ6LOGP.

z/OS *Použití CSQ6USGP*

Toto téma slouží jako reference pro nastavení parametrů systému pomocí CSQ6USGP .

Pomocí CSQ6USGP můžete řídit záznam použití produktu.

Výchozí parametry pro CSQ6USGP jsou zobrazeny v souboru Tabulka 62 na stránce 921. Pokud potřebujete změnit některou z těchto hodnot, podívejte se na podrobný popis parametrů.

Upozornění: Žádný z těchto parametrů nelze změnit pomocí příkazu SET SYSTEM.

Tabulka 62. Výchozí hodnoty parametrů CSQ6USGP

Parametr	Popis	Výchozí hodnota
QMGRPROD	Produkt, pro který má být zaznamenáno využití správce front	Prázdný
AMSPROD	Produkt, pro který má být zaznamenáno využití produktu Advanced Message Security (AMS)	Prázdný

QMGRPROD

Určuje produkt, pro který má být zaznamenáno využití správce front.

Zadejte jednu z následujících možností:

MQ

Využití správce front je zaznamenáno jako samostatný produkt IBM MQ for z/OS s ID produktu 5655-MQ9.

VUE

Využití správce front je zaznamenáno jako samostatný produkt IBM MQ for z/OS Value Unit Edition (VUE) s ID produktu 5655-VU9.

ADVANCEDVUE

Použití správce front je zaznamenáno jako součást produktu IBM MQ Advanced for z/OS Value Unit Edition s ID produktu 5655-AV1.

AMSPROD

Není-li tento parametr nastaven, adresní prostor AMS se nespustí a bude vydána zpráva CSQY024I .

Uvádí produkt, pro který má být zaznamenáno využití produktu Advanced Message Security , pokud se používá.

Zadejte jednu z následujících možností:

AMS

Využití AMS je zaznamenáno jako samostatný produkt Advanced Message Security for z/OS s ID produktu 5655-AM9.

ROZŠÍŘENÝ

Využití AMS je zaznamenáno jako součást produktu IBM MQ Advanced for z/OS s ID produktu 5655-AV9.

ADVANCEDVUE

Využití AMS je zaznamenáno jako součást produktu IBM MQ Advanced for z/OS Value Unit Edition s ID produktu 5655-AV1.

Další informace o záznamu využití produktu viz Informace o produktu vytváření sestav .

Související odkazy

“Použití CSQ6SYSP” na stránce 900
Toto téma slouží jako reference pro nastavení systémových parametrů pomocí CSQ6SYSP.

“Použití CSQ6LOGP” na stránce 909
Toto téma slouží jako reference pro určení voleb protokolování pomocí CSQ6LOGP.

z/OS *Přizpůsobit parametry inicializátoru kanálu*

Pomocí příkazu ALTER QMGR upravte inicializátor kanálu tak, aby vyhovoval vašim požadavkům.

- *Opakujte tuto úlohu pro každého IBM MQ správce front podle potřeby.*
- *Tuto úlohu musíte provést při migraci z předchozí verze.*

Způsob fungování distribuovaného řazení do front řídí řada atributů správce front. Nastavte tyto atributy pomocí příkazu MQSC ALTER QMGR. Ukázka inicializační datové sady thlqual.SCSQPROC(CSQ4INYG) obsahuje některá nastavení, která můžete upravit. Další informace viz ALTER QMGR.

Hodnoty těchto parametrů jsou zobrazeny jako posloupnost zpráv při každém spuštění inicializátoru kanálu.

Vztah mezi adaptéry, dispečery a maximálním počtem kanálů

Parametry ALTER QMGR CHIADAPS a CHIDISPS definují počet řídicích bloků úloh (TCB) používaných inicializátorem kanálu. CHIADAPS (adaptér) TCB se používají k provedení volání rozhraní API IBM MQ do správce front. CHIDISPS (dispečer) TCB se používají k volání do komunikační sítě.

Parametr MAXCHL ALTER QMGR ovlivňuje distribuci kanálů přes dispečerské TCB.

CHIDISPS

Pokud máte malý počet kanálů, použijte výchozí hodnotu.

Jedna úloha pro každý procesor optimalizuje výkon systému. Vzhledem k tomu, že úlohy dispečera jsou náročné na CPU, je principem udržovat co nejméně úloh, aby byl minimalizován čas potřebný k nalezení a spuštění podprocesů.

Systém CHIDISPS (20) je vhodný pro systémy s více než 100 kanály. Není pravděpodobné, že by v případě CHIDISPS (20) existovala významná nevýhoda, pokud se jedná o více dispečerských TCB, než je nezbytné.

Pokud máte více než 1000 kanálů, jako vodítko povolte jeden dispečer pro každých 50 aktuálních kanálů. Například uveďte CHIDISPS (40) pro obsluhu až 2000 aktivních kanálů.

Používáte-li protokol TCP/IP, je maximální počet dispečerů používaných pro kanály TCP/IP 100, a to i v případě, že v parametru CHIDISPS zadáte větší hodnotu.

CHIADAPS

Každé volání rozhraní IBM MQ API do správce front je nezávislé na ostatních a lze je provést na libovolném adaptéru TCB. Volání používající trvalé zprávy mohou trvat mnohem déle než volání pro přechodné zprávy z důvodu vstupu/výstupu protokolu. Proto iniciátor kanálu, který zpracovává velký počet trvalých zpráv v mnoha kanálech, může potřebovat více než výchozích 8 TCB adaptéru pro optimální výkon. To platí zejména v případech, kdy je dosažená velikost dávky malá, protože konec dávkového zpracování také vyžaduje vstup/výstup protokolu a kde jsou použity kanály tenkého klienta.

Navržená hodnota pro produkční prostředí je CHIADAPS (30). Použití více než tohoto je nepravděpodobné, že by poskytlo významný dodatečný přínos, a je nepravděpodobné, že by byla nějaká významná nevýhoda v tom, že by CHIADAPS (30) měl, pokud je to více adaptérů TCB, než je nutné.

MAXCHL

Každý kanál je při spuštění kanálu přidružen ke konkrétnímu dispečerovi TCB a zůstává přidružen k tomuto TCB, dokud se kanál nezastaví. Mnoho kanálů může sdílet každý TCB. MAXCHL se používá k rozložení kanálů mezi dostupné dispečerské TCB. První (MIN ((MAXCHL/CHIDISPS)) , 10) kanály, které se mají spustit, jsou přidruženy k prvnímu dispečerovi TCB atd., dokud se všechny dispečerové bloky TCB nepoužívají.

To má za následek malý počet kanálů a velký MAXCHL, že kanály nejsou rovnoměrně distribuovány mezi dispečery. Pokud například nastavíte CHIDISPS (10) a ponecháte MAXCHL na výchozí hodnotě 200, ale pouze 50 kanálů, pět dispečerů bude přidruženo k 10 kanálům a pět bude nevyužito.

Doporučujeme nastavit MAXCHL na počet kanálů, které mají být skutečně použity, kde se jedná o malé pevné číslo.

Změníte-li tuto vlastnost správce front, musíte také zkontrolovat vlastnosti správce front ACTCHL, LU62CHLa TCPCHL, abyste se ujistili, že jsou hodnoty kompatibilní. Úplný popis těchto vlastností a jejich vztah naleznete v tématu Parametry správce front .

Nastavení prostředí z/OS UNIX System Services pro iniciátory kanálů

Inicializátor kanálu (CHINIT) používá podprocesy OMVS. Přezkoumejte konfigurační parametry OMVS před vytvořením nového CHINIT nebo úpravou počtu dispečerů nebo SSLTASKS.

Každý CHINIT používá 3 + CHIDISP + SSLTASKS OMVS podprocesy. Ty přispívají k celkovému počtu podprocesů OMVS použitých v oblasti LPAR a k počtu podprocesů použitých ID uživatele spuštěné úlohy CHINIT.

Můžete použít **D OMVS,L** a zkontrolovat aktuální využití, využití vysoké vody a systémový limit MAXPROCSYS (maximální počet procesů, které systém povoluje).

Pokud přidáváte nový CHINIT nebo zvyšujete hodnoty CHIDISPS nebo SSLTASKS, musíte vypočítat nárůst podprocesů a přezkoumat dopad na hodnoty MAXPROCSYS. Pomocí příkazu **SETOMVS** můžete dynamicky měnit MAXPROCSYS nebo aktualizovat hodnotu knihovny parametrů BPXPRCxx nebo obojí.

Parametr OMVS MAXPROCUSER je počet podprocesů OMVS, které může mít jeden uživatel OMVS se stejným UID. Podprocesy se započítávají do této hodnoty. Máte-li tedy 2 CHINITS se stejným ID uživatele spuštěné úlohy, s 10 dispečery a 3 SSLTASKS, pak jsou 2 * (3 +10 + 3) = 32 podprocesů pro identifikátor OMVS.

Výchozí hodnotu MAXPROCUSER můžete zobrazit zadáním příkazu **D OMVS,O** a pomocí příkazu **SETOMVS** můžete dynamicky změnit hodnotu parametru MAXPROCUSER nebo aktualizovat hodnotu knihovny parametrů BPXPRCxx nebo obojí.

Tuto hodnotu můžete přepsat na základě počtu uživatelů pomocí RACF příkazu **ALTUSER userid OMVS(PROCUSERMAX(nnnn))** nebo ekvivalentu.

Chcete-li spustit inicializátor kanálu, zadejte následující příkaz:

```
START CHINIT
```

Chcete-li se ujistit, že byl inicializátor kanálu úspěšně spuštěn, zkontrolujte, že v protokolu úloh xxxxCHIN(ssidCHIN) není chyba ICH408I .

Související pojmy

“Nastavení adaptérů Batch, TSO a RRS” na stránce 923
Zpřístupněte adaptéry aplikacím přidáním knihoven do příslušných zřetězení STEPLIB. Chcete-li obstarávat výpisy paměti SNAP vydané adaptérem, přidělte název DDDName CSQSNAP. Zvažte použití CSQBDEFV pro zlepšení přenositelnosti vašich aplikačních programů

Související odkazy

Datové záznamy statistiky inicializátoru kanálu

z/OS *Nastavení adaptérů Batch, TSO a RRS*

Zpřístupněte adaptéry aplikacím přidáním knihoven do příslušných zřetězení STEPLIB. Chcete-li obstarávat výpisy paměti SNAP vydané adaptérem, přidělte název DDDName CSQSNAP. Zvažte použití CSQBDEFV pro zlepšení přenositelnosti vašich aplikačních programů

- *Tuto úlohu opakujte pro každého IBM MQ správce front podle potřeby.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*

Chcete-li adaptéry zpřístupnit dávkovým aplikacím a dalším aplikacím pomocí dávkových připojení, přidejte do zřetězení STEPLIB pro dávkovou aplikaci následující knihovny IBM MQ :

- thlqual.SCSQANL *x*

- thlqual.SCSQAUTH

kde *x* je jazykový dopis pro váš národní jazyk. (Nemusíte to dělat, pokud jsou knihovny v LPA nebo v seznamu odkazů.)

Pro aplikace TSO přidejte knihovny do zřetězení STEPLIB v přihlašovací proceduře TSO nebo je aktivujte pomocí příkazu TSO TSOLIB.

Pokud adaptér zjistí neočekávanou chybu systému IBM MQ , vydá aplikaci příkaz z/OS SNAP dump to DDDname CSQSNAP a aplikaci vydá kód příčiny `MQRC_UNEXPECTED_ERROR` .Není-li příkaz CSQSNAP DD v JCL aplikace nebo není-li CSQSNAP přidělen k datové sadě v rámci TSO, neprovádí se žádný výpis. Pokud k tomu dojde, můžete zahrnout příkaz CSQSNAP DD do JCL aplikace nebo přidělit CSQSNAP k datové sadě v rámci TSO a znovu spustit aplikaci. Vzhledem k tomu, že některé problémy jsou občasné, doporučuje se do kódu JCL aplikace zahrnout příkaz CSQSNAP nebo přidělit architekturu CSQSNAP datové sadě v přihlašovací proceduře TSO za účelem zachycení příčiny selhání v době, kdy k němu došlo.

Dodávaný program CSQBDEFV zlepšuje přenositelnost vašich aplikačních programů. V prostředí CSQBDEFV můžete zadat název správce front nebo skupiny sdílení front, k níž chcete být připojeni, a nikoli jej zadat ve volání `MQCONN` nebo `MQCONNX` v aplikačním programu. Můžete vytvořit novou verzi CSQBDEFV pro každého správce front nebo skupinu sdílení front. Postupujte takto:

1. Zkopírujte program assembleru IBM MQ CSQBDEFV z thlqual.SCSQASMS do uživatelské knihovny.
2. Dodaný program obsahuje výchozí název subsystému CSQ1. Tento název můžete uchovat pro testování a ověření instalace. V případě produkčních subsystémů můžete změnit název NAME=CSQ1 na jednoznakový až čtyřznakový název subsystému, nebo můžete použít CSQ1.

   Používáte-li skupiny sdílení front, můžete místo názvu CSQ1zadat název skupiny sdílení front. Pokud tak učiníte, program vydá požadavek na připojení k aktivnímu správci front v rámci této skupiny.
3. Sestavte a upravte program tak, aby produkoval zaváděcí modul CSQBDEFV. Pro sestavení zahrňte knihovnu thlqual.SCSQMACS do zřetězení SYSLIB; použijte parametry linkování `RENT,AMODE=31,RMODE=ANY`. To se zobrazí v ukázkovém JCL v thlqual.SCSQPROC(CSQ4DEFV). Poté zahrňte zaváděcí knihovnu do z/OS Batch nebo TSO STEPLIB před thlqual.SCSQAUTH.

Související pojmy

“Nastavení operací a ovládacích panelů” na stránce 924

Chcete-li nastavit operace a ovládací panely, musíte nejprve nastavit knihovny, které obsahují požadované panely, EXEC, zprávy a tabulky. Chcete-li to provést, musíte vzít v úvahu, která funkce národního jazyka má být použita pro panely. Po provedení tohoto úkonu můžete volitelně aktualizovat hlavní nabídku ISPF pro operace IBM MQ a ovládací panely a změnit nastavení funkčních kláves.

z/OS *Nastavení operací a ovládacích panelů*

Chcete-li nastavit operace a ovládací panely, musíte nejprve nastavit knihovny, které obsahují požadované panely, EXEC, zprávy a tabulky. Chcete-li to provést, musíte vzít v úvahu, která funkce národního jazyka má být použita pro panely. Po provedení tohoto úkonu můžete volitelně aktualizovat hlavní nabídku ISPF pro operace IBM MQ a ovládací panely a změnit nastavení funkčních kláves.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*

Nastavení knihoven

Chcete-li nastavit operace a ovládací panely IBM MQ , postupujte takto:

1. Ujistěte se, že všechny knihovny obsažené ve vašich zřetězeních jsou buď ve stejném formátu (F, FB, V, VB) a mají stejnou velikost bloku, nebo jsou v pořadí podle klesající velikosti bloku. V opačném případě může dojít k problémům při pokusu o použití těchto panelů.
2. Zahrňte knihovnu thlqual.SCSQEXEC do zřetězení SYSEXEC nebo SYSPROC nebo ji aktivujte pomocí příkazu TSO ALTLIB. Tato knihovna, která je během instalace přidělena s formátem záznamu 80 s pevným blokem, obsahuje požadované EXEC.

Je vhodnější vložit knihovnu do zřetězení SYSEXEC. Chcete-li jej však vložit do SYSPROC, musí mít knihovna délku záznamu 80 bajtů.

3. Přidejte thlqual.SCSQAUTH a thlqual.SCSQANLx do přihlašovací procedury TSO STEPLIB nebo ji aktivujte pomocí příkazu TSO TSOLIB, pokud není v seznamu odkazů nebo LPA.
4. Knihovny panelu IBM MQ můžete buď trvale přidat do svého nastavení knihovny ISPF , nebo jim povolit dynamické nastavení při použití panelů. Pro dřívější volbu je třeba provést následující:
   a. Zahrňte knihovnu obsahující definice operací a ovládacích panelů do zřetězení ISPPLIB. Název je thlqual.SCSQPNLx, kde x je písmeno jazyka pro váš národní jazyk.
   b. Zahrňte knihovnu obsahující požadované tabulky do zřetězení ISPTLIB. Název je thlqual.SCSQTBLx, kde x je písmeno jazyka pro váš národní jazyk.
   c. Zahrňte knihovnu obsahující požadované zprávy do zřetězení ISPMLIB. Název je thlqual.SCSQMSGx, kde x je písmeno jazyka pro váš národní jazyk.
   d. Zahrňte knihovnu obsahující požadované zaváděcí moduly do zřetězení ISPLLIB. Název této knihovny je thlqual.SCSQAUTH.

   Pro druhou volbu použijte příkaz z/OS LIBDEF . Odkaz na různá klíčová slova, která můžete použít, naleznete v části Příklady .
5. Otestujte, zda máte přístup k panelům IBM MQ z panelu Příkazový procesor TSO. Obvykle se jedná o volbu 6 v nabídce ISPF/PDF Primary Options. Název EXEC, který spustíte, je CSQOREXX.Neexistují žádné parametry, které by bylo možné určit, pokud jste knihovny IBM MQ trvale vložili do nastavení ISPF , jako v kroku 4. Pokud nemáte, použijte následující:

```
CSQOREXX thlqual langletter
```

   kde `langletter` je písmeno označující národní jazyk, který má být použit:

   C
   Zjednodušená čínština

   E
   U.S. Angličtina (malá i velká písmena)

   F
   Francouzština

   K
   Japonština

   U
   U.S. Angličtina (velká písmena)

Aktualizace nabídky ISPF

Můžete aktualizovat hlavní nabídku ISPF , abyste umožnili přístup k operacím a ovládacím panelům IBM MQ z ISPF. Požadované nastavení pro & ZSEL je:

```
CMD(%CSQOREXX thlqual langletter)
```

Informace o `thlqual` a `langletter`viz krok “5” na stránce 925.

Další podrobnosti viz příručka a odkaz *z/OS: ISPF Dialog Developer's Guide and Reference*.

Aktualizace funkčních kláves a nastavení příkazů

Ke změně funkčních kláves a nastavení příkazů používaných panely můžete použít běžné procedury ISPF . Identifikátor aplikace je CSQO.

Toto se však nedoporučuje, protože informace nápovědy nejsou aktualizovány tak, aby odrážely provedené změny.

Související pojmy

"Zahrnout člena formátování výpisu paměti IBM MQ" na stránce 926
Chcete-li mít možnost formátovat výpisy paměti systému IBM MQ pomocí interaktivního systému pro řízení problémů (IPCS), musíte aktualizovat některé systémové knihovny.

z/OS *Zahrnout člena formátování výpisu paměti IBM MQ*

Chcete-li mít možnost formátovat výpisy paměti systému IBM MQ pomocí interaktivního systému pro řízení problémů (IPCS), musíte aktualizovat některé systémové knihovny.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.*
- *Tuto úlohu musíte provést při migraci z předchozí verze.*

Chcete-li být schopni formátovat výpisy paměti IBM MQ pomocí systému IPCS (Interactive Problem Control System), zkopírujte datovou sadu thlqual.SCSQPROC(CSQ7IPCS) do SYS1.PARMLIB. Tuto datovou sadu byste neměli upravovat.

Pokud jste upravili proceduru TSO pro IPCS, thlqual.SCSQPROC(CSQ7IPCS) lze zkopírovat do libovolné knihovny v definici IPCSPARM. Další informace viz příručka *z/OS MVS IPCS User's Guide* .

Do zřetězení ISPPLIB musíte také zahrnout knihovnu thlqual.SCSQPNLA .

Chcete-li zpřístupnit formátovací programy výpisu paměti pro vaši relaci TSO nebo úlohu IPCS, musíte také zahrnout knihovnu thlqual.SCSQAUTH do zřetězení STEPLIB nebo ji aktivovat pomocí příkazu TSO TSOLIB (i když je již v seznamu odkazů nebo LPA).

Související pojmy

"Potlačit informační zprávy" na stránce 926
Váš systém IBM MQ může vytvořit velký počet informačních zpráv. Můžete zabránit odesílání vybraných zpráv na konzolu nebo do protokolu tištěné kopie.

z/OS *Potlačit informační zprávy*

Váš systém IBM MQ může vytvořit velký počet informačních zpráv. Můžete zabránit odesílání vybraných zpráv na konzolu nebo do protokolu tištěné kopie.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ.*
- *Tuto úlohu nemusíte provádět při migraci z předchozí verze.*

Pokud je systém IBM MQ intenzivně využíván a mnoho kanálů se zastavuje a spouští, odešle se velký počet informačních zpráv do konzoly z/OS a do protokolu tištěné kopie. Most IBM MQ - IMS a správce vyrovnávací paměti mohou také vytvářet velký počet informačních zpráv.

V případě potřeby můžete některé z těchto zpráv konzoly potlačit pomocí seznamu zařízení pro zpracování zpráv z/OS určeného členy MPFLSTxx systému SYS1.PARMLIB. Zprávy, které zadáte, se stále objeví v protokolu tištěné kopie, ale ne na konzole.

Ukázka `thlqual.SCSQPROC(CSQ4MPFL)` zobrazuje navrhovaná nastavení pro MPFLSTxx. Další informace viz MPFLSTxx (seznam zařízení pro zpracování zpráv) .

Chcete-li potlačit vybrané informační zprávy v protokolu tištěné kopie, můžete použít uživatelskou proceduru instalace z/OS IEAVMXIT. Pro požadované zprávy můžete nastavit následující bitové přepínače ON:

CTXTRDTM
Odstraňte zprávu.

Zpráva se nezobrazuje na konzolách ani není přihlášena v tištěné podobě.

CTXTESJL
Potlačit z protokolu úlohy.

Zpráva nepřejde do protokolu úlohy JES.

CTXTNWTP
Neprovádějte zpracování WTP.

Zpráva není odeslána na terminál TSO nebo do datové sady systémových zpráv dávkové úlohy.

Poznámka:

1. Úplné podrobnosti o ostatních parametrech naleznete v tématu Uživatelské procedury instalace MVS.
2. Nedoporučuje se potlačovat jiné zprávy než ty, které jsou uvedeny v navrhovaném seznamu potlačení, CSQ4MPFL.

Kromě toho můžete zadat další parametr:

EXCLMSG
Uvádí seznam zpráv, které mají být vyloučeny z jakéhokoli protokolu.

Zprávy v tomto seznamu nejsou odesílány na konzolu z/OS a do protokolu tištěné kopie. Další informace viz EXCLMSG v souboru “Použití CSQ6SYSP” na stránce 900 .

Související úlohy

“Testování správce front v systému z/OS” na stránce 941
Pokud jste upravili nebo migrovali svého správce front, můžete jej otestovat spuštěním programů pro ověření instalace a některých ukázkových aplikací dodávaných s produktem IBM MQ for z/OS.

z/OS Konfigurace skupiny sdílení front

Chcete-li pro vysokou dostupnost používat sdílené fronty, použijte tato témata jako průvodce konfigurací skupiny sdílení front krok za krokem.

Po dokončení kroků v této části procesu pro nastavení systému IBM MQ for z/OS byste měli “Přizpůsobení modulu systémových parametrů” na stránce 898 přidat data skupiny sdílení front. Musíte upravit CSQ6SYSP tak, aby uváděli parametr QSGDATA.

z/OS *Nastavení prostředí Db2*

Pokud používáte skupiny sdílení front, musíte vytvořit požadované objekty Db2 úpravou a spuštěním řady ukázkových úloh.

Nastavení prostředí Db2

Musíte vytvořit a svázat požadované objekty Db2 přizpůsobením a spuštěním řady ukázkových úloh.

- Tuto úlohu opakujte pro každou skupinu sdílení dat Db2 .
- Při migraci z předchozí verze musíte provést kroky `bind` a `grant` .
- Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.

  Chcete-li později používat skupiny sdílení front, proveďte tuto úlohu v tuto chvíli.

IBM MQ poskytuje dvě ekvivalentní sady úloh. Ty s předponou CSQ45 jsou pro kompatibilitu se staršími verzemi produktu IBM MQ a pro použití s produktem IBM MQ verze 11 a dřívějšími. Pokud nastavujete novou skupinu sdílení dat s produktem Db2 V12 nebo novějším, doporučuje se používat úlohy s předponou CSQ4X , protože tyto úlohy využívají novější funkce Db2 pro dynamickou změnu velikosti a univerzální tabulkové prostory (UTS).

Pro každou novou skupinu sdílení dat Db2 je třeba provést následující kroky. Všechny ukázky JCL jsou v thlqual.SCSQPROC.

1. Upravte a proveďte ukázku JCL CSQ4XCSG a vytvořte paměťovou skupinu, která má být použita pro databázi IBM MQ , tabulkové prostory a tabulky.
2. Upravte a proveďte ukázku JCL CSQ4XCDB , abyste vytvořili databázi, kterou mají používat všichni správci front, kteří se připojují k této skupině sdílení dat Db2 .

3. Upravte a proveďte ukázku JCL CSQ4XCTS a vytvořte tabulkové prostory, které obsahují tabulky správce front a inicializátoru kanálu používané pro skupiny sdílení front.
4. Upravte a proveďte ukázku JCL CSQ4XCTB pro vytvoření 15 tabulek Db2 a přidružených indexů. Neměňte žádné názvy řádků nebo atributy.
5. Upravte a proveďte ukázku JCL CSQ45BPL tak, aby svázala plány Db2 pro správce front, obslužné programy a inicializátor kanálu.
6. Upravte a proveďte ukázku JCL CSQ45GEX , abyste udělili oprávnění k provádění plánům pro ID uživatelů, která jsou používána správcem front, obslužnými programy a inicializátorem kanálu. ID uživatelů pro správce front a inicializátor kanálu jsou ID uživatelů, pod nimiž jsou spouštěny jejich spuštěné procedury úloh. ID uživatelů pro obslužné programy jsou ID uživatelů, pod kterými lze dávkové úlohy odeslat.

   Názvy příslušných plánů jsou uvedeny v následující tabulce.

Uživatel	**Plány (LTS)**	**Plány (CD)**
Správce front	CSQ5A 930, CSQ5C 930, CSQ5D 930, CSQ5K 930, CSQ5L 930, CSQ5M 930, CSQ5P 930, CSQ5R 930, CSQ5S 930, CSQ5T 930, CSQ5U 930, CSQ5W 930	CSQ5A 9X0, CSQ5C 9X0, CSQ5D 9X0, CSQ5K 9X0, CSQ5L 9X0, CSQ5M 9X0, CSQ5P 9X0, CSQ5R 9X0, CSQ5S 9X0, CSQ5T 9X0, CSQ5U 9X0, CSQ5W 9X0
Funkce SDEFS dávkového obslužného programu CSQUTIL	CSQ52 930	CSQ52 9X0
CSQ5PQSG a obslužné programy dávek CSQJUCNV	CSQ5B 930	CSQ5B 9X0
Obslužný program služby CSQUZAP	CSQ5Z 930	CSQ5Z 9X0

V případě selhání během nastavení produktu Db2 lze upravit a provést následující úlohy:

- CSQ45DTB pro zrušení tabulek a indexů.
- CSQ4XDTS pro zrušení tabulkových prostorů.
- CSQ4XDDB pro zrušení databáze.
- CSQ4XDSG pro zrušení paměťové skupiny.

Poznámka: Pokud tyto úlohy selžou kvůli problému se zamykáním systému Db2 , je to pravděpodobně kvůli soupeření o prostředek systému Db2 , zejména pokud je systém silně využíván. Úlohy znovu odešlete později. Je vhodnější spouštět tyto úlohy, když je systém lehce používán nebo uveden do klidového stavu.

Další informace o nastavení produktu Db2viz Db2 Administration v části *Db2 pro z/OS 12.0.0* .

Informace o velikostech tabulek Db2 naleznete v části Plánování v z/OS .

Související pojmy

“Nastavení prostředku Coupling Facility” na stránce 929
Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front ve skupině sdílení front (QSG) v datové sadě zásad CFRM (coupling facility Resource Management) pomocí IXCMIAPU.

z/OS Nastavení prostředku Coupling Facility

Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front ve skupině sdílení front (QSG) v datové sadě zásad CFRM (coupling facility Resource Management) pomocí IXCMIAPU.

Další informace o obslužném programu IXCMIAPU naleznete v tématu Obslužný program pro administrativní data .

- Tuto úlohu opakujte pro každou skupinu sdílení front.
- Možná budete muset provést tuto úlohu při migraci z předchozí verze.
- Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.

  Chcete-li později používat skupiny sdílení front, proveďte tuto úlohu v tuto chvíli.

Všechny struktury pro skupinu sdílení front začínají názvem skupiny sdílení front. Definujte následující struktury:

- Administrativní struktura s názvem *qsg-name* CSQ_ADMIN. Tuto strukturu používá samotný produkt IBM MQ a neobsahuje žádná uživatelská data.
- Struktura systémové aplikace s názvem *qsg-name* CSQSYSAPPL. Tuto strukturu používají fronty systému IBM MQ k ukládání informací o stavu.
- Jedna nebo více struktur používaných k uchování zpráv pro sdílené fronty. Ty mohou mít libovolný název, který vyberete, až 16 znaků dlouhý.
  - První čtyři znaky musí být název skupiny sdílení front. (Je-li název skupiny sdílení front kratší než čtyři znaky, musí být doplněn na čtyři znaky symboly @.)
  - Pátý znak musí být abecední a následující znaky mohou být abecední nebo číselné. Tato část názvu (bez názvu skupiny sdílení front) je určena pro název CFSTRUCT při definování sdílené fronty nebo objektu struktury prostředku CF.

  V názvech struktur používaných k uchování zpráv pro sdílené fronty lze použít pouze abecední a číselné znaky, nelze použít žádné jiné znaky (například znak _, který se používá v názvu administrativní struktury).

Ukázkové řídicí příkazy pro IXCMIAPU jsou v datové sadě thlqual.SCSQPROC(CSQ4CFRM). Upravte je a přidejte je do úlohy IXCMIAPU pro prostředek Coupling Facility a spusťte jej.

Když jste úspěšně definovali své struktury, aktivujte používanou zásadu CFRM. Chcete-li to provést, zadejte následující příkaz z/OS :

```
SETXCF START,POLICY,TYPE=CFRM,POLNAME= policy-name
```

Informace o plánování struktur prostředku Coupling Facility a jejich velikosti naleznete v tématu Definování prostředků prostředku Coupling Facility.

Související pojmy

“Implementace ovládacích prvků zabezpečení ESM” na stránce 890
Implementujte řízení zabezpečení pro správce front a iniciátor kanálu.

z/OS Nastavení prostředí SMDS

Chcete-li k odlehčování zpráv ve sdílených frontách použít SMDS, nastavte úložné prostředí odlehčování SMDS.

- *Tuto úlohu proveďte pro každého správce front a strukturu ve skupině sdílení front, kterou chcete konfigurovat pro odkládání dat do SMDS.*
- *Chcete-li později konfigurovat další struktury pro odlehčování dat do SMDS, lze tuto úlohu v daném okamžiku provést znovu.*
- *Vynechte tuto úlohu, pokud nepoužíváte skupiny sdílení front.*

Pokud později budete chtít používat skupiny sdílení front, proveďte tuto úlohu v tuto chvíli.

Nastavení prostředí SMDS

1. Odhadněte strukturu a požadavky na prostor datové sady. Viz Aspekty kapacity datové sady sdílených zpráv.
2. Přidělit a předformátovat datové sady. Viz Vytvoření datové sady sdílených zpráv.
3. Při definování struktury prostředku CF na hodnotu IBM MQse ujistěte, že jste definovali CFSTRUCT s CFLEVEL (5) a OFFLOAD (SMDS).

Související pojmy

“Nastavení prostředku Coupling Facility” na stránce 929
Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front ve skupině sdílení front (QSG) v datové sadě zásad CFRM (coupling facility Resource Management) pomocí IXCMIAPU.

z/OS *Přidejte položky IBM MQ do tabulek Db2 .*

Používáte-li skupiny sdílení front, spusťte obslužný program CSQ5PQSG a přidejte položky skupiny sdílení front a položky správce front do tabulek IBM MQ ve skupině sdílení dat Db2 .

- *Tuto úlohu opakujte pro každou IBM MQ skupinu sdílení front a každého správce front.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*
- *Vynechte tuto úlohu, pokud nepoužíváte skupiny sdílení front.*

  Pokud později budete chtít používat skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Spusťte CSQ5PQSG pro každou skupinu sdílení front a pro každého správce front, který má být členem skupiny sdílení front.

Proveďte následující akce v uvedeném pořadí:

1. Přidejte položku skupiny sdílení front do tabulek produktu IBM MQ Db2 pomocí funkce ADD QSG programu CSQ5PQSG . Ukázka je uvedena v souboru thlqual.SCSQPROC(CSQ45AQS).

   Tuto funkci proveďte jednou pro každou skupinu sdílení front, která je definována ve skupině sdílení dat Db2 . Před přidáním všech položek správce front, které odkazují na danou skupinu sdílení front, musí existovat položka skupiny sdílení front.
2. Přidejte položku správce front do tabulek produktu IBM MQ Db2 pomocí funkce ADD QMGR programu CSQ5PQSG . Ukázka je uvedena v souboru thlqual.SCSQPROC(CSQ45AQM).

   Tuto funkci proveďte pro každého správce front, který má být členem skupiny sdílení front.

   Poznámka:

   a. Správce front může být členem pouze jedné skupiny sdílení front.

   b. Aby bylo možné používat skupiny sdílení front, musí být spuštěna služba RRS.

Související pojmy

“Přizpůsobení modulu systémových parametrů” na stránce 898
Modul systémových parametrů IBM MQ řídí prostředí protokolování, archivace, trasování a připojení, která produkt IBM MQ používá ve své činnosti. Je dodán výchozí modul. Měli byste vytvořit svůj vlastní modul systémových parametrů, protože některé parametry, například názvy datových sad, jsou obvykle specifické pro daný server.

z/OS *Implementace ovládacích prvků zabezpečení ESM pro skupinu sdílení front*

Implementujte řízení zabezpečení pro všechny správce front ve skupině sdílení front pro přístup k produktu Db2 a strukturám seznamu prostředku Coupling Facility.

- *Tuto úlohu opakujte pro všechny správce front produktu IBM MQ ve skupině sdílení front.*
- *Možná budete muset provést tuto úlohu při migraci z předchozí verze.*

Ujistěte se, že ID uživatelů přidružená ke správci front, inicializátoru kanálu a obslužným programům mají oprávnění k vytvoření připojení RRSAF ke každému subsystému Db2 , se kterým chcete vytvořit připojení. ID uživatelů pro správce front a inicializátor kanálu jsou ID uživatelů, pod nimiž jsou spouštěny jejich spuštěné procedury úloh.

ID uživatelů pro obslužné programy jsou ID uživatelů, pod kterými lze dávkové úlohy odeslat. Profil RACF , ke kterému ID uživatele vyžaduje přístup READ, je `Db2ssid.RRSAF` ve třídě prostředků DSNR.

ID uživatelů přidružených ke každému správci front ve skupině sdílení front musí mít přidělenu odpovídající úroveň přístupu ke strukturám seznamu prostředku Coupling Facility. Třída RACF je FACILITY.

Následující ID uživatelů vyžadují přístup ALTER:

- ID správce front pro profil `IXLSTR.structure-name`
- ID uživatele, který spouští CSQ5PQSG

Související pojmy

“Implementace ovládacích prvků zabezpečení ESM” na stránce 890
Implementujte řízení zabezpečení pro správce front a iniciátor kanálu.

z/OS Konfigurace produktu Advanced Message Security for z/OS

Tato témata použijte jako průvodce konfigurací produktu Advanced Message Security (AMS) krok za krokem.

Než začnete

Před zahájením konfigurace produktu AMSse ujistěte, že byly provedeny následující kroky konfigurace správce front:

1. Přidejte modul CSQ0DRTM do LPA, jak je popsáno v tématu “Aktualizovat seznam odkazů z/OS a LPA” na stránce 879.
2. Přidejte položku pro CSQ0DSRV do tabulky vlastností programu z/OS (PPT), jak je popsáno v tématu “Aktualizovat tabulku vlastností programu z/OS” na stránce 883.
3. Zahrňte člena CSQ4INSM do zřetězení CSQINP2 procedury spuštěné úlohy správce front, jak je popsáno v tématu “Upravit vstupní datové sady inicializace” na stránce 891.
4. Povolte AMS pomocí atributu AMSPROD. Další podrobnosti viz Záznam využití produktu s produkty IBM MQ for z/OS.

Jak pokračovat dále

Nakonfigurujte zásady pro fronty chráněné produktem AMS. Zásady zabezpečení jsou popsány v tématu Administrace Advanced Message Security zásad zabezpečení.

V části Příklad konfigurací v systému z/OSjsou uvedeny příklady konfigurací systému AMS .

z/OS *Vytvořit procedury pro Advanced Message Security*

Každý subsystém IBM MQ , který má být konfigurován pro použití Advanced Message Security (AMS), vyžaduje ke spuštění adresního prostoru AMS katalogizovanou proceduru. Můžete vytvořit vlastní knihovnu procedur dodanou s produktem IBMnebo ji použít.

Postup

1. Zkopírujte ukázkovou proceduru spuštěné úlohy *thlqual*.SCSQPROC (CSQ4AMSM) do svého SYS1.PROCLIB nebo, pokud nepoužíváte SYS1.PROCLIB, vaše knihovna procedur. Pojmenujte proceduru xxxxAMSM, kde xxxx je název vašeho subsystému IBM MQ . Například CSQ1AMSM by byla AMS spuštěná procedura úlohy pro správce front CSQ1.
2. Vytvořte kopii pro každý subsystém IBM MQ , který budete používat.

3. Přizpůsobte procedury vašim požadavkům pomocí pokynů v ukázkové proceduře CSQ4AMSM. Můžete také použít symbolické parametry v JCL, chcete-li povolit úpravu procedury při jejím spuštění.
4. Zkontrolujte a volitelně změňte parametry předané úloze AMS pomocí souboru Language Environment ® _CEE_ENVFILE. Ukázka thlqual.SCSQPROC(CSQ40ENV) vypisuje podporované parametry.
5. Opakujte kroky 1 až 4 pro každého správce front IBM MQ .

Jak pokračovat dále

“Nastavení ID uživatele spuštěné úlohy Advanced Message Security” na stránce 932

z/OS Nastavení ID uživatele spuštěné úlohy Advanced Message Security

Úloha Advanced Message Security (AMS) vyžaduje ID uživatele, které umožňuje, aby bylo známé jako proces z/OS UNIX System Services (z/OS UNIX).

Informace o této úloze

Kromě toho uživatelé, jejichž jménem úloha pracuje, musí mít také odpovídající definici UID systému UNIX (ID uživatele) a GID (ID skupiny), aby tito uživatelé byli označováni jako uživatelé systému z/OS UNIX System Services . Další informace o definování z/OS UNIX System Services identifikátorů UID a GID viz *z/OS: RACF Příručka administrátora zabezpečení*serveru zabezpečení.

Přečtěte si téma *z/OS UNIX System Services Plánování* , abyste se ujistili, že rozumíte rozdílům v zabezpečení mezi tradičním UNIX zabezpečením a zabezpečením produktu z/OS UNIX . To vám umožňuje spravovat úlohu Advanced Message Security podle zásad zabezpečení vaší instalace pro implementaci a spouštění privilegovaných procesů z/OS UNIX System Services .

Primární rozdíl mezi tradičním zabezpečením UNIX a zabezpečením z/OS spočívá v tom, že služby jádra podporují dvě úrovně odpovídajících oprávnění: UNIX úroveň a z/OS UNIX úroveň.

V závislosti na zásadách zabezpečení vaší instalace může být úloha Advanced Message Security spuštěna s oprávněním superuživatele (uid (0)) nebo s identitou RACF povolenou pro RACF třídu FACILITY BPX.DAEMON a profily BPX.SERVER , protože tato úloha musí být schopna převzít identitu RACF svých uživatelů.

Je-li použita druhá metoda, nebo jste již aktivovali BPX.DAEMON nebo profily BPX.SERVER , program úlohy Advanced Message Security (thlqual.SCSQAUTH(CSQ0DSRV)) musí být umístěn v knihovnách řízených programem RACF .

Poznámka: Pečlivě vyberte ID uživatele pro tuto úlohu, protože certifikáty příjemce Advanced Message Security jsou načteny do svazku klíčů přidruženého k tomuto ID uživatele. Tato úvaha je diskutována v tématu Použití certifikátů v systému z/OS .

Zde uvedené kroky popisují, jak nastavit uživatele spuštěné úlohy Advanced Message Security . Tyto kroky používají jako příklady příkazy RACF . Pokud používáte jiného správce zabezpečení, měli byste použít ekvivalentní příkazy.

Poznámka: Příklady v této sekci předpokládají, že jste aktivovali zpracování příkazu generického profilu pro třídy RACF STARTED, FACILITY a SURROGAT a kontrolu generického profilu. Další informace o tom, jak produkt RACF zpracovává generické profily, viz *z/OS: RACF Popis příkazového jazyka serveru zabezpečení*.

Postup

1. Definujte uživatele spuštěné úlohy Advanced Message Security pro RACF. Příklady v této sekci používají ID uživatele WMQAMSM.

   ```
   ADDUSER WMQAMSM NAME('AMS user') OMVS (UID(0)) DFLTGRP(group)
   ```

   Vyberte výchozí 'skupinu' podle svých instalačních standardů.

Poznámka: Pokud nechcete udělit oprávnění superuživatele z/OS UNIX (UID (0)), musíte povolit ID uživatele Advanced Message Security pro BPX.DAEMON a BPX.SERVER :

```
PERMIT BPX.DAEMON CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
```

a program úlohy Advanced Message Security (*thlqual*.SCSQAUTH (CSQ0DSRV)) musí být umístěn v knihovně řízené programem RACF .

Chcete-li nastavit program knihovny SCSQAUTH jako řízený, můžete použít následující příkaz:

```
RALTER PROGRAM * ADDMEM('thlqual.SCSQAUTH'//NOPADCHK) -or-
RALTER PROGRAM ** ADDMEM('thlqual.SCSQAUTH'//NOPADCHK)
SETROPTS WHEN(PROGRAM) REFRESH
```

Musíte také povolit řízení programu pro knihovnu národních jazyků (*thlqual*.SCSQANLx), kterou používá úloha Advanced Message Security .

2. Určete, zda je třída RACF STARTED aktivní. Pokud není, aktivujte třídu RACF STARTED:

```
SETROPTS CLASSACT(STARTED)
```

3. Definujte profil spuštěné třídy pro úlohy Advanced Message Security s uvedením ID uživatele, které jste vybrali nebo vytvořili v kroku 1:

```
RDEFINE STARTED qmgrAMSM.* STDATA(USER(WMQAMSM))
```

kde *qmgr* je předpona názvu spuštěné úlohy. Například spuštěná úloha může mít název CSQ1AMSM. V tomto případě byste nahradili *qmgr*AMSM.* za CSQ1AMSM.*.

Spuštěné úlohy AMS musí mít název *qmgr*AMSM.

4. Pomocí příkazu **SETROPTS** RACF obnovte profily tříd RACLISTed STARTED v úložišti:

```
SETROPTS RACLIST(STARTED) REFRESH
```

5. Úloha Advanced Message Security dočasně přebírá identitu ID uživatele hostitele žadatele během zpracování ochrany zpráv produktu IBM MQ . Proto je nezbytné definovat profily ve třídě SURROGAT pro každé ID uživatele, které může vytvářet požadavky.

Pokud je třída RACF SURROGAT aktivní, definování jednoho generického profilu umožní úloze Advanced Message Security převzít identitu libovolného uživatele. Kontrola je ignorována, pokud není třída SURROGAT aktivní. Potřebné profily SURROGAT jsou popsány v tématu *z/OS UNIX System Services Plánování*.

Chcete-li definovat profily ve třídě SURROGAT, postupujte takto:

a) Aktivujte třídu RACF SURROGAT pomocí příkazu RACF SETROPTS:

```
SETROPTS CLASSACT(SURROGAT)
```

b) Aktivujte zpracování generického profilu pro třídu RACF SURROGAT:

```
SETROPTS GENERIC(SURROGAT)
```

c) Aktivujte zpracování příkazu generického profilu pro třídu RACF SURROGAT:

```
SETROPTS GENCMD(SURROGAT)
```

d) Definujte generický profil ve třídě SURROGAT:

```
RDEFINE SURROGAT BPX.SRV.* UACC(NONE)
```

e) Povolte ID uživatele Advanced Message Security pro generický profil třídy SURROGAT:

```
PERMIT BPX.SRV.* CLASS(SURROGAT) ID(WMQAMSM) ACCESS(READ)
```

Poznámka: Můžete definovat konkrétnější profily, chcete-li omezit zpracování specifických uživatelů úlohou Advanced Message Security , jak je popsáno v tématu *z/OS UNIX System Services Plánování*.

Například profil s názvem BPX.SRV.MQUSER1 řídí, zda může úloha AMS převzít identitu ID uživatele MQUSER1.

f) Povolte ID uživatele Advanced Message Security pro prostředek BPX.SERVER (není-li již provedeno v části Vytvoření certifikátů a kroužků klíčů):

```
PERMIT BPX.SERVER CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
```

g) Použijte příkaz **SETROPTS** RACF k aktualizaci profilů tříd spuštěných v úložišti RACLISTed:

```
SETROPTS RACLIST(SURROGAT) REFRESH
SETROPTS RACLIST(FACILITY) REFRESH
```

6. Úloha Advanced Message Security používá prostředky poskytované službami zabezpečení SSL systému z/OS k otevření svazku klíčů spravovaných zařízením SAF. Základní prostředek SAF (System Authorization Facility), který přistupuje k obsahu svazku klíčů, je řízen produktem RACFnebo ekvivalentním správcem zabezpečení.

   Tato služba je volatelnou službou IRRSDL00 (R_datalib). Tato volatelná služba je chráněna stejnými profily, které se používají k ochraně příkazů RACF RACDCERT, které jsou definovány pro třídu RACF FACILITY. Proto musí být ID uživatele Advanced Message Security povoleno pro profily pomocí těchto příkazů:

   a) Pokud jste tak dosud neučinili, definujte generický profil RACF pro třídu FACILITY systému RACF , která chrání příkaz RACDCERT a volatelnou službu IRRSDL00 :

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

   b) Udělte oprávnění k ID uživatele spuštěné úlohy generickému profilu RACF :

```
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID(WMQAMSM) ACC(READ)
```

   Alternativně můžete udělit přístup READ ke svazku klíčů uživatele úlohy datové služby ve třídě RDATALIB následujícím způsobem:

```
PERMIT WMQASMD.DRQ.AMS.KEYRING.LST CLASS(RDATALIB) ID(WMQAMSM) ACC(READ)
```

7. Konfigurovat zabezpečení prostředků:

   a) Uživatel spuštěné úlohy Advanced Message Security vyžaduje oprávnění pro připojení ke správci front jako dávkovou aplikaci.

   Pokud má váš správce front povoleno zabezpečení připojení, udělte oprávnění k úloze AMS pro připojení ke správci front pomocí tohoto příkazu:

```
PERMIT hlq.BATCH CLASS(MQCONN) ID(WMQAMSM) ACC(READ)
```

   kde *hlq* může být buď název skupiny sdílení front správce front, nebo název skupiny sdílení front.

Další informace naleznete v tématu Profily zabezpečení připojení pro dávková připojení.

b) Uživatel spuštěné úlohy Advanced Message Security vyžaduje oprávnění k procházení SYSTEM.PROTECTION.POLICY.QUEUE.

Pokud je ve správci front aktivní zabezpečení fronty, udělte uživateli AMS oprávnění pro přístup k frontě pomocí těchto příkazů:

```
RDEFINE MQQUEUE hlq.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
PERMIT hlq.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE) ID(WMQAMSM) ACCESS(READ)
```

kde *hlq* může být buď název skupiny sdílení front správce front, nebo název skupiny sdílení front.

Pokud správce front používá profily smíšených případů, definujte profil ve třídě MXQUEUE.

Chcete-li spravovat zásady zabezpečení AMS pomocí obslužného programu CSQ0UTIL , potřebují administrátoři přístup pro vložení zpráv do SYSTEM.PROTECTION.POLICY.QUEUE. To se provádí udělením přístupu UPDATE k profilu, který chrání frontu.

Další informace naleznete v tématu Profily pro zabezpečení fronty.

Jak pokračovat dále

“Udělte oprávnění RACDCERT administrátorovi zabezpečení pro Advanced Message Security” na stránce 935

z/OS *Udělte oprávnění RACDCERT administrátorovi zabezpečení pro Advanced Message Security*

Administrátor zabezpečení systému Advanced Message Security vyžaduje oprávnění k vytváření a správě digitálních certifikátů pomocí příkazu RACDCERT.

Procedura

- Identifikujte odpovídající ID uživatele pro tuto roli a udělte oprávnění k použití příkazu RACDCERT. Příklad:

```
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID(admin) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

kde `admin` je ID uživatele vašeho administrátora zabezpečení Advanced Message Security .

Jak pokračovat dále

“Udělit uživatelům oprávnění k prostředkům pro Advanced Message Security” na stránce 935

z/OS *Udělit uživatelům oprávnění k prostředkům pro Advanced Message Security*

Uživatelé produktu Advanced Message Security vyžadují příslušná oprávnění k prostředkům.

Informace o této úloze

Uživatelé systému Advanced Message Security , tj. uživatelé, kteří vkládají nebo získávají Advanced Message Security chráněné zprávy, vyžadují:

- Segment OMVS přidružený k jejich ID uživatele
- Oprávnění pro IRR.DIGTCERT.LISTRING nebo RDATALIB
- Oprávnění pro profily CSFSERV a CSFKEYS třídy ICSF
- Oprávnění k vložení do SYSTEM.PROTECTION.ERROR.QUEUE

Úloha Advanced Message Security dočasně přebírá identitu svých klientů; to znamená, že se tato úloha chová jako náhrada z/OS ID uživatele Advanced Message Security během zpracování zpráv produktu IBM MQ do front, které jsou chráněny produktem Advanced Message Security.

Aby mohla úloha převzít identitu z/OS uživatele, ID uživatele klienta z/OS musí mít definovaný segment OMVS přidružený ke svému profilu uživatele.

Jako administrativní pomůcka produkt RACF poskytuje schopnost definovat výchozí segment OMVS, který může být přidružen k profilům uživatelů a skupin produktu RACF . Tato předvolba se použije, pokud ID uživatele nebo profil skupiny z/OS nemá explicitně definovaný segment OMVS. Pokud plánujete mít velký počet uživatelů, kteří používají produkt Advanced Message Security, můžete zvolit použití této předvolby, spíše než explicitní definování segmentu OMVS pro každého uživatele.

Příručka *z/OS: Security Server RACF Security Administrator's Guide* obsahuje podrobný postup pro definování výchozích segmentů OMVS. Přezkoumejte proceduru, jak je popsána v této příručce, abyste určili, zda definice výchozích segmentů OMVS v profilech uživatele a skupiny produktu RACF odpovídá vaší instalaci.

Postup

1. Udělte oprávnění READ pro IRR.DIGTCERT.LISTRING ve třídě FACILITY:
   - Chcete-li udělit oprávnění READ IRR IRR.DIGTCERT.LISTRING ve třídě FACILITY všem uživatelům zadejte tento příkaz:

     ```
     RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(READ)
     ```

   - Chcete-li udělit oprávnění READ IRR IRR.DIGTCERT.LISTRING ve třídě FACILITY na základě počtu uživatelů zadejte tento příkaz:

     ```
     PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(userid) ACCESS(READ)
     ```

     kde ID uživatele je jméno uživatele Advanced Message Security .
   - Alternativně použijte třídu RDATALIB k udělení přístupu ke specifickým kroužkům klíčů. Oprávnění RDATALIB mají přednost před IRR.DIGTCERT.LISTRING . Příklad:

     ```
     PERMIT user.DRQ.AMS.KEYRING.LST CLASS(RDATALIB) ID(user) ACC(READ)
     ```

2. Pokud používáte certifikáty spravované ICSF a soukromé klíče, uživatelé produktu Advanced Message Security vyžadují přístup k určitým profilům třídy CSFSERV a CSFKEYS. Tento přístup je podrobně popsán v následující tabulce:

   Tabulka 63. Požadovaný uživatelský přístup k profilům CSFSERV a CSFKEYS

Třída	**Profil**	**Oprávnění**
CSFSERV	CSFDSG	READ (čtení)
CSFSERV	CSFPKE	READ (čtení)
CSFSERV	CSFPKD	READ (čtení)
CSFSERV	CSFDSV	READ (čtení)
CSFKEYS	Popisek PKDS ICSF	READ (čtení)

3. Aplikace, které provádějí operace ve frontách s definovanými zásadami systému AMS , potřebují přístup pro vkládání zpráv do systému SYSTEM.PROTECTION.ERROR.QUEUE. Udělte přístup pro vložení do fronty pomocí těchto příkazů:

   ```
   RDEFINE MQQUEUE hlq.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
   PERMIT hlq.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE) ID(userId) ACCESS(UPDATE)
   ```

   kde *hlq* může být buď název skupiny sdílení front názvu správce front, nebo *userID* je ID uživatele aplikace.

Jak pokračovat dále

“Vytvořit svazky klíčů pro Advanced Message Security” na stránce 937

z/OS *Vytvořit svazky klíčů pro Advanced Message Security*

Certifikáty používané produktem Advanced Message Security (AMS) pro podepisování a šifrování jsou uloženy ve svazku klíčů SAF produktu z/OS . Před použitím produktu AMSje třeba vytvořit tyto svazky klíčů a certifikáty.

Informace o této úloze

Produkt Advanced Message Security přistupuje k certifikátům v následujících kroužcích klíčů:

- Jeden svazek klíčů vlastněný uživatelem adresního prostoru AMS .
- Svazky klíčů vlastněné jednotlivými uživateli, kteří odesílají nebo přijímají zprávy ve frontách s definovanými zásadami AMS .

Všechny tyto svazky klíčů musí mít název `drq.ams.keyring`.

Další informace o kroužcích klíčů a certifikátech používaných produktem AMSa ukázkový scénář naleznete v tématu Použití certifikátů v systému z/OS.

Postupujte takto, chcete-li vytvořit svazky klíčů požadované produktem AMSa připojit certifikáty ke svazky klíčů. Před spuštěním AMSmusíte vytvořit svazek klíčů vlastněný uživatelem AMS adresního prostoru. Můžete vytvořit svazky klíčů vlastněné uživateli, kteří odesílají nebo přijímají zprávy kdykoli.

Postup

1. Zadáním následujícího příkazu vytvořte svazek klíčů vlastněný uživatelem adresního prostoru AMS :

   ```
   RACDCERT ID(amsUser) ADDRING(drq.ams.keyring)
   ```

   kde *amsUser* je ID uživatele adresního prostoru AMS .
2. Vytvořte svazek klíčů pro každého uživatele, který odesílá nebo přijímá zprávy chráněné produktem AMS , zadáním příkazu v kroku 1 pro každé ID uživatele.
3. Připojte certifikát certifikační autority (CA) pro vydavatele uživatelských certifikátů k svazku klíčů vlastněnému ID uživatele adresního prostoru AMS . Spusťte následující příkaz:

   ```
   RACDCERT ID(amsUser) CONNECT(CERTAUTH LABEL('caLabel') RING(drq.ams.keyring))
   ```

   kde *amsUser* je ID uživatele adresního prostoru AMS a *caLabel* je popisek certifikátu CA.

   Pokud používáte produkt RACF jako svého CA a potřebujete vytvořit certifikát certifikační autority, postupujte podle příkladu v části Definování lokálního certifikátu certifikační autority.
4. Pokud k šifrování zpráv ve frontách chráněných produktem AMSpoužíváte zásady zabezpečení ochrany soukromí nebo důvěrnosti, připojte certifikáty příjemců zpráv ke svazku klíčů vlastněnému ID uživatele adresního prostoru AMS . Spusťte následující příkaz:

   ```
   RACDCERT ID(amsUser) CONNECT(ID(userId) LABEL('certLabel')
   RING(drq.ams.keyring) USAGE(SITE))
   ```

   kde *amsUser* je ID uživatele adresního prostoru AMS , *userId* je příjemce zprávy a *certLabel* je popisek certifikátu uživatele.

   Atribut `USAGE(SITE)` zabraňuje přístupu k soukromému klíči ve svazku klíčů.

   Pokud vytváříte vlastní certifikáty pomocí produktu RACF, postupujte podle příkladu v části Vytvoření digitálního certifikátu se soukromým klíčem a vytvořte certifikát.
5. Připojte certifikáty každého uživatele, který odesílá nebo přijímá zprávy chráněné produktem AMS , ke svazku klíčů vlastněnému uživatelem. Certifikát musí být připojen jako výchozí certifikát v svazku klíčů. Spusťte následující příkaz:

```
RACDCERT ID(userId) CONNECT(ID(userId) LABEL('certLabel')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

kde *userId* je uživatel, který odesílá nebo přijímá zprávy, a *certLabel* je popisek uživatelského certifikátu.

Notes:

a. Kroky “2” na stránce 937 a “5” na stránce 937 nejsou vyžadovány, pokud aplikace otevře frontu pouze pro výstup a odešle zprávy do front chráněných zásadou důvěrnosti AMS .

b. Kroky “2” na stránce 937 a “5” na stránce 937 nejsou vyžadovány, pokud aplikace otevře frontu pouze pro vstup/procházení a přijme zprávy z front chráněných zásadou integrity AMS .

Jak pokračovat dále

“PovolitAdvanced Message Security” na stránce 938

z/OS *PovolitAdvanced Message Security*

Schopnost zásad zabezpečení pro správce front je řízena parametrem SPLCAP v modulu systémových parametrů.

Informace o této úloze

Chcete-li povolit funkci Advanced Message Security (AMS) pro jednoho správce front, postupujte takto.

Tato úloha vyžaduje, abyste změnili modul systémových parametrů. Další informace o vytváření a přizpůsobení modulu systémových parametrů naleznete v části “Přizpůsobení modulu systémových parametrů” na stránce 898 .

Postup

1. Nastavte **SPLCAP** na YES v CSQ6SYSP. Další informace o makru CSQ6SYSP naleznete v části “Použití CSQ6SYSP” na stránce 900 .
2. Nastavte **AMSPROD** na AMS, ADVANCED nebo ADVANCEDVUE v závislosti na vašem licenčním oprávnění. Další informace o makru CSQ6USGP naleznete v tématu použití CSQ6USGP .
3. Znovu zkompilujte modul parametrů systému.
4. Restartujte správce front s aktualizovaným modulem systémových parametrů. Adresní prostor AMS se spustí automaticky při spuštění správce front.

z/OS Konfigurace serveru mqweb

Tato témata použijte jako příručku krok za krokem pro konfiguraci serveru mqweb.

Související úlohy

“Konfigurace IBM MQ Console a REST API” na stránce 786

Server mqweb, který je hostitelem IBM MQ Console a REST API , je poskytován s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh, například konfiguraci zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny dostupné volby konfigurace.

z/OS *Vytvoření serveru mqweb*

Pokud jste nainstalovali produkt IBM MQ for z/OS UNIX System Services Web Componentsa chcete použít server IBM MQ Consolenebo REST API, musíte vytvořit a upravit server mqweb.

Než začnete

Před spuštěním skriptu **crtmqweb** pro vytvoření serveru mqweb nastavte proměnnou prostředí JAVA_HOME tak, aby odkazovala na 64bitovou verzi produktu Java ve vašem systému.

IBM MQ Console a administrative REST API vyžadují SYSTEM.REST.REPLY.QUEUE , která se má vytvořit. Vytvořte tuto frontu pomocí ukázky **CSQ4INSG** v souboru “Upravit vstupní datové sady inicializace” na stránce 891.

Upozornění: Pokud při spouštění serveru mqweb narazíte na chybovou zprávu CWWKG0014E, která se zobrazí v následujícím výstupu:

```
     Launching mqweb (MQM MVS/ESA V9 R2.0/wlp...) (en_US)
                ÝAUDIT   ¨ CWWKE0001I: The server mqweb has been
launched.
                ÝWARNING ¨ CWWKF0009W: The server has not been configured to install any
features.
                ÝAUDIT   ¨ CWWKF0011I: The mqweb server is ready to run a smarter planet.
The mqweb server started in 6.348 seconds.
                ÝERROR   ¨ CWWKG0014E: The configuration parser detected an XML syntax
error while parsing the root of the configuration and the referenced configuration
documents.
                                Error: An invalid XML character (Unicode: 0x4c) was found
in the prolog of the document.
                                 File: file:<your filepath>/servers/mqweb/server.xml Line:
1 Column: 1
```

měli byste zkontrolovat nastavení z/OS AUTOCVT (automaticky převádět soubory z jedné kódové sady na jinou) a upravit hodnotu podle potřeby provedením jedné z následujících možností.

V terminálu USS:

Zadejte příkaz: echo **$_BPXK_AUTOCVT** , abyste zobrazili hodnotu této proměnné prostředí. Není-li proměnná prostředí definována, nezobrazí se žádná hodnota.

Chcete-li nastavit proměnnou prostředí, prohlédněte si téma Proměnné prostředí _BPXK.

Po celém systému:

Příklad 6 na Zobrazení stavu z/OS UNIX System Services (OMVS) ukazuje, jak zobrazit hodnotu celosystémového příkazu AUTOCVT v BPXPRMxx.

Chcete-li nastavit proměnnou prostředí na celý systém, použijte příkaz AUTOCVT v BPXPRMxx.

Je-li proměnná prostředí _BPXX_AUTOCVT nastavena v terminálu USS, přepíše celosystémové nastavení příkazu AUTOCVT v BPXPRMxx.

Informace o této úloze

- Tuto úlohu proveďte jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ Console nebo REST API.
- Chcete-li použít administrative REST API, potřebujete server mqweb pro každou spuštěnou verzi produktu IBM MQ . Pokud například používáte servery IBM MQ 9.3.0, 9.2.5 a 9.2.0, potřebujete tři různé servery mqweb.
- Při migraci z předchozí verze může být nutné aktualizovat nebo upravit konfiguraci serveru.

IBM MQ Console a REST API vyžadují vytvoření jednoho serveru WebSphere Liberty s názvem mqweb.

Všechny soubory konfigurace serveru a soubory protokolu jsou uloženy v uživatelském adresáři Liberty .

Server mqweb musí být konfigurován s ID produktu (PID), pod kterým je spuštěn. PID je nastaveno při vytvoření serveru mqweb. Použijte stejný identifikátor PID, který se používá ke spuštění lokálních správců front, ke kterým se server mqweb připojuje.

Poznámka: Pokud jsou lokální správci front spouštěni pod více různými identifikátory PID, vyberte jeden z nich, pod kterým má být spuštěn server mqweb.

Další informace o identifikátorech PID a způsobu jejich použití v systému z/OSnaleznete v tématu Záznam o využití produktu s IBM MQ for z/OS produkty.

Je možné změnit PID, pod kterým je server mqweb spuštěn, po jeho vytvoření, pomocí příkazu setmqweb .

Chcete-li vytvořit server mqweb, postupujte takto:

Postup

1. Rozhodněte, pod kterým PID je spuštěn server mqweb.
2. Vyberte vhodné umístění pro uživatelský adresář Liberty .

   ID uživatele, pod kterým je spuštěn server mqweb, potřebuje přístup pro čtení a zápis k tomuto uživatelskému adresáři a jeho obsahu. Vzhledem k tomu, že tento uživatelský adresář obsahuje soubory protokolu, kromě konfigurace serveru vytvořte tento adresář v odděleném systému souborů.

   Poznámka: Při spuštění serveru mqweb existuje významné množství diskového vstupu/výstupu. Chcete-li zkrátit dobu potřebnou ke spuštění serveru mqweb, ujistěte se, že souborový systém IBM MQ instalace z/OS UNIX i souborový systém adresáře uživatelů Liberty buď zohledňují prostředí sysplex, nebo jsou lokálně připojeny k systému, kde je spuštěn server mqweb.
3. V produktu z/OS UNIX System Serviceszměňte aktuální pracovní adresář na `PathPrefix/web/bin` zadáním následujícího příkazu:

   ```
   cd PathPrefix/web/bin
   ```

   kde *PathPrefix* je instalační cesta IBM MQ for z/OS UNIX System Services Components .
4. Vytvořte uživatelský adresář Liberty , který obsahuje definici serveru mqweb šablony, spuštěním skriptu **crtmqweb** .

   Formát příkazu **crtmqweb** je:

   ```
   crtmqweb user_directory -p pid_value
   ```

   kde:

   adresář_uživatele
   Je adresář uživatelů Liberty rozhodnutý v kroku “2” na stránce 940. Tento parametr je volitelný. Není-li tento parametr uveden, použije se výchozí Liberty uživatelský adresář `/var/mqm/web/installation1` .

   hodnota pid_value
   Označuje PID, pod kterým je spuštěn server mqweb. Tento PID je ten, který jste vybrali v kroku “1” na stránce 940. *pid_value* je jedna z následujících hodnot:

   MQ
   Server mqweb je spuštěn pod PID IBM MQ for z/OS (5655-MQ9).

   VUE
   Server mqweb je spuštěn pod PID IBM MQ for z/OS Value Unit Edition (VUE) (5655-VU9).

   ADVANCEDVUE
   Server mqweb je spuštěn pod PID IBM MQ Advanced for z/OS VUE (5655-AV1),

   Chcete-li například vytvořit server mqweb s uživatelským adresářem Liberty `/usr/mqweb` a PID IBM MQ Advanced for z/OS VUE (5655-AV1), spusťte tento příkaz:

   ```
   ./crtmqweb /usr/mqweb -p ADVANCEDVUE
   ```
5. Změňte vlastnictví adresářů a souborů v uživatelském adresáři Liberty tak, aby patřily k ID uživatele a skupině, pod kterými je spuštěn server mqweb, pomocí příkazu:

   ```
   chown -R userid:group path
   ```

   Chcete-li skupině udělit přístup pro zápis k cestě, zadejte příkaz:

   ```
   chmod -R 770 path
   ```

Jak pokračovat dále

“Vytvoření procedury pro server mqweb” na stránce 941

Související úlohy

“Konfigurace IBM MQ Console a REST API” na stránce 786

Server mqweb, který je hostitelem IBM MQ Console a REST API , je poskytován s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh, například konfiguraci zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny dostupné volby konfigurace.

z/OS *Vytvoření procedury pro server mqweb*

Pokud jste nainstalovali agenta IBM MQ for z/OS UNIX System Services Web Componentsa chcete použít agenta IBM MQ Consolenebo agenta REST API, musíte vytvořit katalogizovanou proceduru pro spuštění serveru mqweb. Server mqweb je server Liberty , který je hostitelem serverů IBM MQ Console a REST API.

- Tuto úlohu musíte provést jednou pro každý systém z/OS , kde chcete spustit IBM MQ Console nebo REST API.
- Potřebujete server mqweb pro každou spuštěnou verzi produktu IBM MQ . Například spuštěná úloha s názvem MQWB0910 pro správce front v IBM MQ for z/OS 9.1.0 a spuštěná úloha s názvem MQWB0905 pro správce front v IBM MQ for z/OS 9.0.5.

  Máte-li v systému z/OS pouze jednoho správce front, můžete spustit jednu spuštěnou úlohu serveru Liberty a změnit knihovny, které používá při migraci správce front.
- Při migraci z předchozí verze může být nutné katalogizovanou proceduru upravit.

Chcete-li vytvořit katalogizovaný postup, postupujte takto:

1. Zkopírujte ukázkovou proceduru spuštěné úlohy `thlqual.SCSQPROC(CSQ4WEBS)` do knihovny procedur.

   Postup pojmenujte podle standardů vašeho podniku.

   Například `MQWB0910`označuje, že se jedná o katalogizovanou proceduru pro server IBM MQ for z/OS 9.1.0 mqweb.
2. Přizpůsobte proceduru vašim požadavkům pomocí pokynů v ukázkové proceduře CSQ4WEBS.

   Všimněte si, že uživatelský adresář Liberty je adresář určený při spuštění skriptu **crtmqweb** pro vytvoření definice serveru mqweb.

   Podrobnosti viz “Vytvoření serveru mqweb” na stránce 938.

   Poznámka: Při úpravách členu se ujistěte, že jste zadali **Caps off** , protože soubor má malá písmena.
3. Autorizujte proceduru ke spuštění pod vaším externím správcem zabezpečení.
4. Tento adresní prostor lze klasifikovat pomocí správce zátěže IBM Workload Manager (WLM).

   Server mqweb je aplikace IBM MQ a uživatelé interaktivně spolupracují s touto aplikací. Aplikace nemusí mít ve WLM vysokou důležitost a třída služeb **STCUSER** může být vhodná.

Další kroky

Dokončete konfiguraci serveru mqweb podle pokynů v části “Základní konfigurace pro server mqweb” na stránce 787 .

Související úlohy

“Konfigurace IBM MQ Console a REST API” na stránce 786
Server mqweb, který je hostitelem IBM MQ Console a REST API , je poskytován s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh, například konfiguraci zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny dostupné volby konfigurace.

z/OS Testování správce front v systému z/OS

Pokud jste upravili nebo migrovali svého správce front, můžete jej otestovat spuštěním programů pro ověření instalace a některých ukázkových aplikací dodávaných s produktem IBM MQ for z/OS.

Informace o této úloze

Po instalaci a úpravě produktu IBM MQ for z/OSmůžete pomocí dodaného programu pro ověření instalace CSQ4IVP1potvrdit, že je produkt IBM MQ for z/OS v provozu.

Základní ověřovací program instalace CSQ4IVP1 testuje nesdílené fronty a ověřuje základní IBM MQ bez použití ukázek jazyka C, COBOL nebo CICS .

Po spuštění základního ověření instalace můžete testovat sdílené fronty pomocí CSQ4IVP1 s různými frontami a také testovat, zda jsou produkt Db2 a prostředek Coupling Facility správně nastaveny. Chcete-li potvrdit, že je distribuované řazení do front funkční, můžete použít dodaný program pro ověření instalace CSQ4IVPX,

CSQ4IVP1 je dodáván jako zaváděcí modul a poskytuje sadu ukázkových procedurálních aplikací jako zdrojové moduly, které demonstrují typická použití rozhraní MQI (Message Queue Interface). Tyto zdrojové moduly můžete použít k testování různých prostředí programovacích jazyků. Pomocí dodaného ukázkového kódu JCL můžete zkompilovat a propojit-upravit kteroukoli z ostatních ukázek, které jsou vhodné pro vaši instalaci.

Procedura

- Informace o tom, jak testovat správce front v systému z/OS, naleznete v následujících dílčích tématech:
  - “Spuštění základního ověřovacího programu instalace” na stránce 942
  - “Testování skupin sdílení front” na stránce 946
  - “Testování distribuovaných front” na stránce 947
  - “Testování programů v jazycích C, C + +, COBOL, PL/I a CICS s produktem IBM MQ for z/OS” na stránce 950

Související pojmy

IBM MQ for z/OS koncepce

Související úlohy

Plánování prostředí IBM MQ na systému z/OS

“Konfigurace správců front v systému z/OS” na stránce 871
Pomocí těchto pokynů můžete konfigurovat správce front v systému IBM MQ for z/OS.

Správa serveruIBM MQ for z/OS

z/OS Spuštění základního ověřovacího programu instalace

Po instalaci a úpravě produktu IBM MQmůžete pomocí dodaného programu pro ověření instalace CSQ4IVP1potvrdit, že je produkt IBM MQ v provozu.

Základní ověřovací program instalace je dávkový sestavovací proces IVP, který ověřuje základní IBM MQ bez použití ukázek C, COBOL nebo CICS .

Dávkový modul sestavení IVP je upraven pomocí odkazu SMP/E a zaváděcí moduly jsou dodávány v knihovně thlqual.SCSQLOAD.

Po dokončení kroku SMP/E APPLY i kroků přizpůsobení spusťte proces IVP dávkového sestavení.

Další podrobnosti naleznete v těchto oddílech:

- Přehled aplikace CSQ4IVP1
- Příprava na spuštění CSQ4IVP1
- Spuštění CSQ4IVP1
- Kontrola výsledků CSQ4IVP1

Přehled aplikace CSQ4IVP1

CSQ4IVP1 je dávková aplikace, která se připojuje k vašemu subsystému IBM MQ a provádí tyto základní funkce:

- Problémy IBM MQ volání
- Komunikuje s příkazovým serverem
- Ověřuje, zda je spouštění aktivní
- Generuje a odstraňuje dynamickou frontu.
- Ověřuje zpracování vypršení platnosti zprávy.
- Ověřuje zpracování potvrzení zprávy

Příprava ke spuštění CSQ4IVP1

Před spuštěním CSQ4IVP1:

1. Zkontrolujte, zda jsou položky IVP ve zřetězení datové sady CSQINP2 ve spouštěcím programu správce front. Položky IVP jsou dodávány ve členu thlqual.SCSQPROC(CSQ4IVPQ). Pokud ne, přidejte definice dodané v thlqual.SCSQPROC(CSQ4IVPQ) do zřetězení CSQINP2 . Pokud je správce front aktuálně spuštěn, je třeba jej restartovat, aby se tyto definice mohly projevit.
2. Ukázkový soubor JCL, CSQ4IVPR, nezbytný ke spuštění programu pro ověření instalace, je v knihovně thlqual.SCSQPROC.

   Upravte soubor JCL CSQ4IVPR pomocí kvalifikátoru vysoké úrovně pro knihovny IBM MQ , národního jazyka, který chcete použít, názvu správce front IBM MQ se čtyřmi znaky a cíle pro výstup úlohy.
3. Aktualizujte soubor RACF , abyste povolili CSQ4IVP1 přístup k jeho prostředkům, pokud je aktivní zabezpečení IBM MQ .

   Chcete-li spustit CSQ4IVP1 , když je povoleno zabezpečení IBM MQ , potřebujete ID uživatele RACF s oprávněním pro přístup k objektům. Podrobnosti o definování prostředků v systému RACFnaleznete v tématu Nastavení zabezpečení v systému z/OS . ID uživatele, který spouští proces IVP, musí mít následující přístupové oprávnění:

Oprávnění	Profil	Třída
READ (čtení)	ssid.DISPLAY.PROCESS	MQCMDS
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.REPLY.MODEL	MQQUEUE
AKTUALIZOVAT	ssid.CSQ4IVP1.**	MQQUEUE
READ (čtení)	ssid.BATCH	MQCONN

   Tyto požadavky předpokládají, že je aktivní veškeré zabezpečení produktu IBM MQ . Příkazy RACF pro aktivaci zabezpečení systému IBM MQ jsou uvedeny v části Obrázek 101 na stránce 944. Tento příklad předpokládá, že název správce front je CSQ1 a ID uživatele, který spustil ukázku CSQ4IVP1 , je TS101.

```
RDEFINE MQCMDS CSQ1.DISPLAY.PROCESS
PERMIT CSQ1.DISPLAY.PROCESS CLASS(MQCMDS) ID(TS101) ACCESS(READ)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.INPUT
PERMIT CSQ1.SYSTEM.COMMAND.INPUT CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.REPLY.MODEL
PERMIT CSQ1.SYSTEM.COMMAND.REPLY.MODEL CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.CSQ4IVP1.**
PERMIT CSQ1.CSQ4IVP1.** CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQCONN CSQ1.BATCH
PERMIT CSQ1.BATCH CLASS(MQCONN) ID(TS101) ACCESS(READ)
```

Obrázek 101. Příkazy RACF pro CSQ4IVP1

Spuštění CSQ4IVP1

Po provedení těchto kroků spusťte správce front. Pokud je správce front již spuštěn a změnili jste CSQINP2, musíte jej zastavit a restartovat.

Proces IVP je spuštěn jako dávková úloha. Přizpůsobte zakázkový list tak, aby splňoval požadavky na odeslání vaší instalace.

Kontrola výsledků CSQ4IVP1

Proces IVP je rozdělen do 10 fází; každá fáze musí být před spuštěním další fáze dokončena s nulovým kódem dokončení. Proces IVP vygeneruje sestavu s výpisem:

- Název správce front, ke kterému se připojují.
- Jednořádková zpráva zobrazující kód dokončení a kód příčiny vrácený z každé fáze.
- Jednořádková informační zpráva, kde je to vhodné.

Ukázková sestava je k dispozici v adresáři Obrázek 102 na stránce 946 .

z/OS Vysvětlení kódů příčiny a dokončení naleznete v tématu IBM MQ for z/OS zprávy, dokončení a kódy příčiny.

Některé fáze mají více než jedno volání IBM MQ a v případě selhání je vydána zpráva označující specifické volání IBM MQ , které vrátilo selhání. Pro některé fáze také IVP vkládá vysvětlující a diagnostické informace do pole komentářů.

Úloha IVP požaduje výlučné řízení určitých objektů správce front, a proto by měla být v systému s jedním podprocesem. Neexistuje však žádné omezení počtu spuštění IVP pro vašeho správce front.

Funkce prováděné každou fází jsou:

Fáze 1
Připojte se ke správci front zadáním volání rozhraní API MQCONN .

Fáze 2
Určete název vstupní fronty systémových příkazů, kterou používá příkazový server k načtení zpráv požadavků. Tato fronta přijímá požadavky na zobrazení z fáze 5.

Chcete-li to provést, posloupnost volání je:

1. Zadáním volání MQOPEN s názvem správce front otevřete objekt správce front.
2. Zadejte volání MQINQ a zjistěte název vstupní fronty systémového příkazu.
3. Zadejte volání MQINQ a zjistěte informace o různých přepínačích událostí správce front.
4. Zadáním volání MQCLOSE zavřete objekt správce front.

Po úspěšném dokončení této fáze se v poli komentáře zobrazí název vstupní fronty systémového příkazu.

Fáze 3
Otevřete inicializační frontu pomocí volání **MQOPEN** .

Tato fronta je otevřena v této fázi v očekávání zprávy spouštěče, která je výsledkem odpovědi příkazového serveru na požadavek z fáze 5. Fronta musí být otevřena pro vstup, aby splňovala spouštěcí kritéria.

Fáze 4
Vytvořte trvalou dynamickou frontu pomocí CSQ4IVP1.MODEL jako model. Dynamická fronta má stejné atributy jako model, ze kterého byla vytvořena. To znamená, že při zápisu odpovědí z požadavku příkazového serveru ve fázi 5 do této fronty se do inicializační fronty otevřené ve fázi 3 zapíše zpráva spouštěče.

Po úspěšném dokončení této fáze je v poli komentáře uveden název trvalé dynamické fronty.

Fáze 5
Zadejte požadavek MQPUT1 do fronty příkazů příkazového serveru.

Do vstupní fronty systémového příkazu se zapíše zpráva typu MQMT_REQUEST, která požaduje zobrazení procesu CSQ4IVP1. Deskriptor zprávy pro zprávu určuje trvalou dynamickou frontu vytvořenou ve fázi 4 jako frontu pro odpověď příkazového serveru.

Fáze 6
Zadejte požadavek **MQGET** z inicializační fronty. V této fázi je pro inicializační frontu otevřenou ve 3. fázi vydán příkaz GET WAIT s intervalem 1 minuty. Očekává se, že vrácená zpráva bude zprávou spouštěče generovanou zprávami odezvy příkazového serveru, které se zapisují do fronty pro odpověď.

Fáze 7
Odstraňte trvalou dynamickou frontu vytvořenou ve fázi 4. Vzhledem k tomu, že fronta stále obsahuje zprávy, je použita volba MQCO_PURGE_DELETE.

Fáze 8

1. Otevřete dynamickou frontu.
2. MQPUT zprávu s nastaveným intervalem vypršení platnosti.
3. Počkejte na vypršení platnosti zprávy.
4. Pokus o MQGET zprávu s vypršenou platností.
5. MQCLOSE-fronta.

Fáze 9

1. Otevřete dynamickou frontu.
2. MQPUT zprávu.
3. Vydejte příkaz MQCMIT k potvrzení aktuální pracovní jednotky.
4. MQGET-zpráva.
5. Zadejte příkaz MQBACK pro vrácení zprávy zpět.
6. MQGET stejnou zprávu a ujistěte se, že počet vrácení je nastaven na 1.
7. Chcete-li zavřít frontu, zadejte příkaz MQCLOSE.

Fáze 10
Odpojte se od správce front pomocí **MQDISC**.

Po spuštění IVP můžete odstranit všechny objekty, které již nepotřebujete.

Pokud se IVP nespustí úspěšně, zkuste každý krok ručně, abyste zjistili, která funkce selhává.

```
DATE : 2005.035                IBM MQ for z/OS - V6           PAGE : 0001
INSTALLATION VERIFICATION PROGRAM
PARAMETERS ACCEPTED. PROGRAM WILL CONNECT TO : CSQ1
,OBJECT QUALIFER : CSQ4IVP1
INSTALLATION VERIFICATION BEGINS :
STAGE 01 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR BRIDGE EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS EXCP FOR CHANNEL EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR SSL EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR INHIBITED EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR LOCAL EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR PERFORMENCE EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR REMOTE EVENTS
STAGE 02 INFO: QMGR EVENT SWITCH IS OFF FOR START/STOP EVENTS
STAGE 02 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 SYSTEM.COMMAND.INPUT
STAGE 03 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 04 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 CSQ4IVP1.BAB9810EFEAC8980
STAGE 05 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 06 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 07 COMPLETE. COMPCODE : 0000 REASON CODE : 0000
STAGE 08 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 CSQ4IVP1.BAB9810F0070E645
STAGE 09 COMPLETE. COMPCODE : 0000 REASON CODE : 0000 CSQ4IVP1.BAB9812BA8706803
STAGE 10 COMPLETE. COMPCODE : 0000 REASON CODE : 0000>>>>>>>>>>   END OF REPORT   <<<<<<<<<<
```

Obrázek 102. Ukázková sestava z CSQ4IVP1

z/OS Testování skupin sdílení front

Základní ověřovací program instalace CSQ4IVP1 testuje nesdílené fronty.

Položku CSQ4IVP1 lze použít bez ohledu na to, zda je správce front členem skupiny sdílení front či nikoli. Po spuštění základního IVP můžete testovat sdílené fronty pomocí ověřovacího programu instalace CSQ4IVP1 s různými frontami. Tímto se také testuje, zda jsou produkt Db2 a prostředek Coupling Facility správně nastaveny.

Příprava na spuštění CSQ4IVP1 pro skupinu sdílení front

Před spuštěním CSQ4IVP1:

1. Přidejte strukturu prostředku Coupling Facility, kterou používá proces IVP, do datové sady zásady CFRM, jak je popsáno v tématu “Nastavení prostředku Coupling Facility” na stránce 929. Dodané ukázky používají strukturu s názvem APPLICATION1, ale můžete ji změnit, pokud chcete.
2. Zkontrolujte, zda jsou položky IVP ve zřetězení datové sady CSQINP2 ve spouštěcím programu správce front. Položky IVP jsou dodávány ve členu thlqual.SCSQPROC(CSQ4IVPG). Pokud nejsou, přidejte definice dodané v souboru thlqual.SCSQPROC(CSQ4IVPG) do zřetězení CSQINP2 . Pokud je správce front aktuálně spuštěn, je třeba jej restartovat, aby se tyto definice mohly projevit.
3. V případě potřeby změňte název struktury prostředku Coupling Facility použité v souboru thlqual.SCSQPROC(CSQ4IVPG).
4. Ukázkový soubor JCL, CSQ4IVPS, nezbytný ke spuštění programu pro ověření instalace pro skupinu sdílení front, je v knihovně thlqual.SCSQPROC.

   Upravte JCL CSQ4IVPS pomocí kvalifikátoru vyšší úrovně pro knihovny IBM MQ , národního jazyka, který chcete použít, názvu správce front IBM MQ se čtyřmi znaky a cíle pro výstup úlohy.
5. Aktualizujte soubor RACF , abyste povolili CSQ4IVP1 přístup k jeho prostředkům, pokud je aktivní zabezpečení IBM MQ .

   Chcete-li spustit CSQ4IVP1 , když je povoleno zabezpečení IBM MQ , potřebujete ID uživatele RACF s oprávněním pro přístup k objektům. Podrobnosti o definování prostředků v systému RACFnaleznete v tématu Nastavení zabezpečení v systému z/OS . ID uživatele, který spouští IVP, musí mít kromě toho, které je nezbytné pro spuštění základního IVP, následující přístupové oprávnění:

Oprávnění	Profil	Třída
AKTUALIZOVAT	ssid.CSQ4IVPG.**	MQQUEUE

Tyto požadavky předpokládají, že je aktivní veškeré zabezpečení produktu IBM MQ . Příkazy RACF pro aktivaci zabezpečení systému IBM MQ jsou uvedeny v části Obrázek 103 na stránce 947. Tento příklad předpokládá, že název správce front je CSQ1 a ID uživatele, který spustil ukázku CSQ4IVP1 , je TS101.

```
RDEFINE MQQUEUE CSQ1.CSQ4IVPG.**
PERMIT CSQ1.CSQ4IVPG.** CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)
```

Obrázek 103. Příkazy RACF pro CSQ4IVP1 pro skupinu sdílení front

Spuštění CSQ4IVP1 pro skupinu sdílení front

Po provedení těchto kroků spusťte správce front. Pokud je správce front již spuštěn a změnili jste CSQINP2, musíte jej zastavit a restartovat.

Proces IVP je spuštěn jako dávková úloha. Přizpůsobte zakázkový list tak, aby splňoval požadavky na odeslání vaší instalace.

Kontrola výsledků CSQ4IVP1 pro skupinu sdílení front

Proces IVP pro skupiny sdílení front pracuje stejným způsobem jako základní proces IVP s tím rozdílem, že vytvořené fronty se nazývají CSQIVPG. *xx*. Postupujte podle pokynů uvedených v části “Kontrola výsledků CSQ4IVP1” na stránce 944 a zkontrolujte výsledky IVP pro skupiny sdílení front.

z/OS Testování distribuovaných front

Pomocí dodaného ověřovacího programu instalace CSQ4IVPXmůžete potvrdit, že distribuované řazení do front je funkční.

Přehled úlohy CSQ4IVPX

CSQ4IVPX je dávková úloha, která spouští inicializátor kanálu a vydává příkaz IBM MQ DISPLAY CHINIT. To ověřuje, zda jsou všechny hlavní aspekty distribuovaného řazení do front funkční, aniž by bylo nutné nastavovat definice kanálů a sítí.

Příprava ke spuštění CSQ4IVPX

Před spuštěním CSQ4IVPX:

1. Ukázkový soubor JCL, CSQ4IVPX, který je nezbytný pro spuštění programu pro ověření instalace, je v knihovně thlqual.SCSQPROC.

   Upravte soubor JCL CSQ4IVPX pomocí kvalifikátoru vysoké úrovně pro knihovny IBM MQ , národního jazyka, který chcete použít, názvu správce front se čtyřmi znaky a cíle pro výstup úlohy.
2. Aktualizujte soubor RACF , abyste povolili CSQ4IVPX přístup k jeho prostředkům, pokud je aktivní zabezpečení IBM MQ . Chcete-li spustit CSQ4IVPX , když je povoleno zabezpečení IBM MQ , potřebujete ID uživatele RACF s oprávněním pro přístup k objektům. Podrobnosti o definování prostředků v systému RACFnaleznete v tématu Nastavení zabezpečení v systému z/OS . ID uživatele, který spouští proces IVP, musí mít následující přístupové oprávnění:

Oprávnění	Profil	Třída
CONTROL	ssid.START.CHINIT a ssid.STOP.CHINIT	MQCMDS
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CSQUTIL.*	MQQUEUE

Oprávnění	Profil	Třída
READ (čtení)	ssid.BATCH	MQCONN
READ (čtení)	ssid.DISPLAY.CHINIT	MQCMDS

Tyto požadavky předpokládají, že profil zabezpečení připojení ssid.CHIN byl definován (jak je uvedeno v části Profily zabezpečení připojení pro inicializátor kanálu) a že je aktivní veškeré zabezpečení IBM MQ . Příkazy RACF , které to mají provést, jsou zobrazeny v souboru Obrázek 104 na stránce 949. Tento příklad předpokládá:

- Název správce front je CSQ1 .
- ID uživatele osoby, která spouští ukázku CSQ4IVPX , je TS101 .
- Adresní prostor inicializátoru kanálu je spuštěn pod ID uživatele CSQ1MSTR .

3. Aktualizujte soubor RACF , abyste povolili adresnímu prostoru inicializátoru kanálu následující přístupové oprávnění:

Oprávnění	Profil	Třída
READ (čtení)	ssid.CHIN	MQCONN
AKTUALIZOVAT	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CHANNEL.INITQ	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CHANNEL.SYNCQ	MQQUEUE
ALTER	ssid.SYSTEM.CLUSTER.COMMAND.QUEUE	MQQUEUE
AKTUALIZOVAT	ssid.SYSTEM.CLUSTER.TRANSMIT.QUEUE	MQQUEUE
ALTER	ssid.SYSTEM.CLUSTER.REPOSITORY.QUEUE	MQQUEUE
CONTROL	ssid.CONTEXT.**	MQADMIN

Příkazy RACF , které to mají provést, jsou také zobrazeny v části Obrázek 104 na stránce 949.

```
RDEFINE MQCMDS CSQ1.DISPLAY.DQM
PERMIT CSQ1.DISPLAY.DQM CLASS(MQCMDS) ID(TS101) ACCESS(READ)

RDEFINE MQCMDS CSQ1.START.CHINIT
PERMIT CSQ1.START.CHINIT CLASS(MQCMDS) ID(TS101) ACCESS(CONTROL)

RDEFINE MQCMDS CSQ1.STOP.CHINIT
PERMIT CSQ1.STOP.CHINIT CLASS(MQCMDS) ID(TS101) ACCESS(CONTROL)

RDEFINE MQQUEUE CSQ1.SYSTEM.COMMAND.INPUT
PERMIT CSQ1.SYSTEM.COMMAND.INPUT CLASS(MQQUEUE) ID(TS101,CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CSQUTIL.*
PERMIT CSQ1.SYSTEM.CSQUTIL.* CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)

RDEFINE MQCONN CSQ1.BATCH
PERMIT CSQ1.BATCH CLASS(MQCONN) ID(TS101) ACCESS(READ)

RDEFINE MQCONN CSQ1.CHIN
PERMIT CSQ1.CHIN CLASS(MQCONN) ID(CSQ1MSTR) ACCESS(READ)

RDEFINE MQQUEUE CSQ1.SYSTEM.CHANNEL.SYNCQ
PERMIT CSQ1.SYSTEM.CHANNEL.SYNCQ CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.COMMAND.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.COMMAND.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(ALTER)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.TRANSMIT.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.TRANSMIT.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQQUEUE CSQ1.SYSTEM.CLUSTER.REPOSITORY.QUEUE
PERMIT CSQ1.SYSTEM.CLUSTER.REPOSITORY.QUEUE CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(ALTER)

RDEFINE MQQUEUE CSQ1.SYSTEM.CHANNEL.INITQ
PERMIT CSQ1.SYSTEM.CHANNEL.INITQ CLASS(MQQUEUE) ID(CSQ1MSTR) ACCESS(UPDATE)

RDEFINE MQADMIN CSQ1.CONTEXT.**
PERMIT CSQ1.CONTEXT.** CLASS(MQADMIN) ID(CSQ1MSTR) ACCESS(CONTROL)
```

Obrázek 104. Příkazy RACF pro CSQ4IVPX

Spuštění CSQ4IVPX

Po provedení těchto kroků spusťte správce front.

Proces IVP je spuštěn jako dávková úloha. Přizpůsobte zakázkový list tak, aby splňoval požadavky na odeslání vaší instalace.

Kontrola výsledků CSQ4IVPX

CSQ4IVPX spustí obslužný program CSQUTIL IBM MQ a vydá tři příkazy MQSC. Výstupní datová sada SYSPRINT by měla vypadat jako Obrázek 105 na stránce 950, i když podrobnosti se mohou lišit v závislosti na atributech správce front.

- Měli byste vidět příkazy **(1)** následované několika zprávami.
- Poslední zpráva každého příkazu by měla být "CSQ9022I ... NORMÁLNÍ DOKONČENÍ" **(2)**.
- Úloha jako celek by měla být dokončena s návratovým kódem nula **(3)**.

```
CSQU000I CSQUTIL IBM MQ for z/OS - V6
CSQU001I CSQUTIL Queue Manager Utility - 2005-05-09 09:06:48
COMMAND
CSQU127I CSQUTIL Executing COMMAND using input from CSQUCMD data set
CSQU120I CSQUTIL Connecting to queue manager CSQ1
CSQU121I CSQUTIL Connected to queue manager CSQ1
CSQU055I CSQUTIL Target queue manager is CSQ1
START CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM138I +CSQ1 CSQMSCHI CHANNEL INITIATOR STARTING
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000000
CSQ9022I +CSQ1 CSQXCRPS ' START CHINIT' NORMAL COMPLETION
(2)
DISPLAY CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM137I +CSQ1 CSQMDDQM DISPLAY CHINIT COMMAND ACCEPTED
CSQN205I  COUNT=   12, RETURN=00000000, REASON=00000000
CSQX830I +CSQ1 CSQXRDQM Channel initiator active
CSQX002I +CSQ1 CSQXRDQM Queue sharing group is QSG1
CSQX831I +CSQ1 CSQXRDQM 8 adapter subtasks started, 8 requested
CSQX832I +CSQ1 CSQXRDQM 5 dispatchers started, 5 requested
CSQX833I +CSQ1 CSQXRDQM 0 SSL server subtasks started, 0 requested
CSQX840I +CSQ1 CSQXRDQM 0 channel connections current, maximum 200
CSQX841I +CSQ1 CSQXRDQM 0 channel connections active, maximum 200,
including 0 paused
CSQX842I +CSQ1 CSQXRDQM 0 channel connections starting,
0 stopped, 0 retrying
CSQX836I +CSQ1 Maximum channels - TCP/IP 200, LU 6.2 200
CSQX845I +CSQ1 CSQXRDQM TCP/IP system name is TCPIP
CSQX848I +CSQ1 CSQXRDQM TCP/IP listener INDISP=QMGR not started
CSQX848I +CSQ1 CSQXRDQM TCP/IP listener INDISP=GROUP not started
CSQX849I +CSQ1 CSQXRDQM LU 6.2 listener INDISP=QMGR not started
CSQX849I +CSQ1 CSQXRDQM LU 6.2 listener INDISP=GROUP not started
CSQ9022I +CSQ1 CSQXCRPS ' DISPLAY CHINIT' NORMAL COMPLETION
(2)
STOP CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM137I +CSQ1 CSQMTCHI STOP CHINIT COMMAND ACCEPTED
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000000
CSQ9022I +CSQ1 CSQXCRPS ' STOP CHINIT' NORMAL COMPLETION
(2)
CSQU057I CSQUCMDS 3 commands read
CSQU058I CSQUCMDS 3 commands issued and responses received, 0 failed
CSQU143I CSQUTIL 1 COMMAND statements attempted
CSQU144I CSQUTIL 1 COMMAND statements executed successfully
CSQU148I CSQUTIL Utility completed, return code=0
(3)
```

Obrázek 105. Příklad výstupu z CSQ4IVPX

z/OS Testování programů v jazycích C, C + +, COBOL, PL/I a CICS s produktem IBM MQ for z/OS

Pomocí ukázkových aplikací dodávaných s produktem IBM MQmůžete testovat jazyky C, C + +, COBOL, PL/I nebo CICS.

Proces IVP (CSQ4IVP1) je dodáván jako zaváděcí modul a poskytuje ukázky jako zdrojové moduly. Tyto zdrojové moduly můžete použít k testování různých prostředí programovacích jazyků.

Další informace o ukázkových aplikacích naleznete v tématu Ukázkové programy pro produkt IBM MQ for z/OS .

z/OS Nastavení komunikace s ostatními správci front v systému z/OS

Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

Informace o této úloze

Chcete-li definovat požadavky na distribuované fronty, musíte definovat následující položky:

- Procedury a datové sady inicializátoru kanálu
- Definice kanálů
- Fronty a další objekty
- Zabezpečení přístupu

Používáte-li skupiny sdílení front, přečtěte si téma Rozdělená řazení do front a skupiny sdílení front.

Další body, které je třeba zvážit při přípravě na nastavení distribuovaného řazení do front pomocí produktu IBM MQ for z/OS, viz “Aspekty použití distribuovaných front v systému z/OS” na stránce 951.

Postup

Chcete-li povolit distribuované řazení do front, postupujte takto:

- Upravte mechanizmus distribuovaného řazení do front a definujte požadované objekty IBM MQ , jak je popsáno v části Definování systémových objektů a “Příprava na přizpůsobení správců front v systému z/OS” na stránce 872.
- Definujte zabezpečení přístupu, jak je popsáno v tématu Aspekty zabezpečení pro inicializátor kanálu v systému z/OS .
- Nastavte komunikaci podle popisu v části “Nastavení komunikace pro z/OS” na stránce 970.

Související pojmy

“nastaveníIBM MQ for z/OS” na stránce 876
Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

Související úlohy

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

z/OS Aspekty použití distribuovaných front v systému z/OS

Body, které je třeba zvážit při přípravě na použití distribuovaných front v systému z/OS.

Používáte-li skupiny sdílení front, přečtěte si téma Rozdělená řazení do front a skupiny sdílení front.

Operátorské zprávy

Vzhledem k tomu, že inicializátor kanálu používá určitý počet asynchronně fungujících dispečerů, mohou se zprávy operátora vyskytovat v protokolu mimo chronologickou posloupnost.

Příkazy pro operace kanálu

Příkazy operace kanálu obvykle zahrnují dvě fáze. Po kontrole syntaxe příkazu a ověření existence kanálu je inicializátoru kanálu odeslán požadavek. Zpráva CSQM134I nebo CSQM137I se odešle vydavateli příkazu, aby označil dokončení první fáze. Po zpracování příkazu inicializátorem kanálu jsou vydavateli příkazu spolu se zprávou CSQ9022I nebo CSQ9023Eodeslány další zprávy označující jeho úspěch nebo jiný úspěch. Jakékoli vygenerované chybové zprávy lze také odeslat na konzolu z/OS .

Všechny příkazy klastru kromě **DISPLAY CLUSQMGR**však pracují asynchronně. Příkazy, které mění atributy objektu, aktualizují objekt a odešlou požadavek na inicializátor kanálu. Příkazy pro práci s klastry jsou kontrolovány na syntaxi a požadavek je odeslán do inicializátoru kanálu. V obou případech je vydavateli příkazu odeslána zpráva CSQM130I , která označuje, že byl odeslán požadavek. Za touto zprávou následuje zpráva CSQ9022I , která označuje, že příkaz byl úspěšně dokončen, v tom, že byl odeslán požadavek. Neoznačuje, že požadavek klastru byl úspěšně dokončen. Požadavky odeslané inicializátoru kanálu jsou zpracovány asynchronně spolu s požadavky klastru přijatými od ostatních členů

klastru. V některých případech musí být tyto požadavky odeslány celému klastru, aby se zjistilo, zda jsou úspěšné nebo ne. Jakékoli chyby jsou nahlášeny produktu z/OS na systému, kde je spuštěn inicializátor kanálu. Nejsou odeslány vydavateli příkazu.

Nedoručeno-fronta zpráv

Obslužná rutina nedoručených zpráv je dodávána s produktem IBM MQ for z/OS. Další informace viz Obslužný program obslužné rutiny fronty nedoručených zpráv (CSQUDLQH).

Používané fronty

MCA pro přijímací kanály mohou ponechat cílové fronty otevřené i v případě, že se zprávy nepřenášejí. Toto chování vede k tomu, že se fronty jeví jako 'používané'.

Změny zabezpečení

Pokud změníte zabezpečený přístup pro ID uživatele, změna se nemusí projevit okamžitě. Další informace naleznete v tématu Aspekty zabezpečení inicializátoru kanálu v adresáři z/OS , Profily pro zabezpečení frontya “Implementace ovládacích prvků zabezpečení ESM” na stránce 890.

Komunikace zastavena-TCP

Je-li protokol TCP z nějakého důvodu zastaven a poté restartován, modul listener TCP systému IBM MQ for z/OS , který čeká na portu TCP, je zastaven.

Automatické opětné připojení kanálu umožňuje iniciátorovi kanálu zjistit, že protokol TCP/IP není k dispozici, a automaticky restartovat modul listener protokolu TCP/IP při návratu protokolu TCP/IP. Tento automatický restart zmírňuje potřebu, aby provozní personál všiml problému s TCP/IP a ručně restartoval modul listener. Když je modul listener mimo akci, iniciátor kanálu může být také použit k zopakování modulu listener v intervalu určeném parametrem LSTRTMR. Tyto pokusy mohou pokračovat, dokud se TCP/IP nevrátí a modul listener se úspěšně automaticky restartuje. Další informace o LSTRTMRnaleznete v části ALTER QMGR a Distribuované zprávy front (CSQX ...).

Komunikace zastavena- LU6.2

Je-li APPC zastaveno, modul listener je také zastaven. V tomto případě se modul listener znovu automaticky pokusí v intervalu LSTRTMR , takže pokud se restartuje APPC, modul listener se také může restartovat.

Pokud Db2 selže, sdílené kanály, které jsou již spuštěny, budou nadále spuštěny, ale všechny nové požadavky na spuštění kanálu selžou. Když se Db2 obnoví, nové požadavky se mohou dokončit.

z/OS Správa automatického restartu (ARM)

Správa automatického restartu (ARM) je funkce obnovy z/OS , která může zlepšit dostupnost specifických dávkových úloh nebo spuštěných úloh (například subsystémů). Může tedy vést k rychlejšímu obnovení produktivní práce.

Chcete-li používat modul ARM, je třeba nastavit správce front a iniciátory kanálů konkrétním způsobem, aby se automaticky restartovali. Další informace naleznete v tématu Použití z/OS správce ARM (Automatic Restart Manager).

Související pojmy

“nastaveníIBM MQ for z/OS” na stránce 876
Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

Související úlohy

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

z/OS Definování objektů IBM MQ na z/OS

V systému z/OSdefinujte objekty IBM MQ pomocí jedné ze vstupních metod příkazu IBM MQ .

Další informace o definování objektů viz “Monitorování a řízení kanálů na systému z/OS” na stránce 954.

Přenosové fronty a spouštěcí kanály

Definujte následující:

- Lokální fronta s použitím XMITQ pro každý odesílající kanál zpráv.
- Definice vzdálené fronty.

  Objekt vzdálené fronty má tři odlišná použití v závislosti na způsobu zadání názvu a obsahu:

  – Definice vzdálené fronty
  – Definice aliasu správce front
  – Definice aliasu fronty pro odpověď

  Tyto tři způsoby jsou uvedeny v tématu Tři způsoby použití objektu definice vzdálené fronty.

Použijte pole TRIGDATA v přenosové frontě ke spuštění uvedeného kanálu. Příklad:

```
DEFINE QLOCAL(MYXMITQ) USAGE(XMITQ) TRIGGER +
INITQ(SYSTEM.CHANNEL.INITQ) TRIGDATA(MYCHANNEL)
DEFINE CHL(MYCHANNEL) CHLTYPE(SDR) TRPTYPE(TCP) +
XMITQ(MYXMITQ) CONNAME('9.20.9.30(1555)')
```

Dodaná ukázka CSQ4INYD poskytuje další příklady nezbytných definic.

z/OS Ztráta konektivity ke struktuře prostředku CF, kde je definována fronta synchronizace pro sdílené kanály, nebo podobné problémy mohou dočasně zabránit spuštění kanálu. Po vyřešení problému, pokud používáte typ spouštěče FIRST a kanál se při spuštění nespustí, musíte spustit kanál ručně. Chcete-li po vyřešení problému automaticky spustit spuštěné kanály, zvažte nastavení atributu TRIGINT správce front na jinou hodnotu než výchozí. Nastavení atributu TRIGINT na jinou hodnotu, než je výchozí, způsobí, že inicializátor kanálu se bude pravidelně pokoušet o spuštění kanálu v době, kdy jsou v přenosové frontě zprávy.

Fronta synchronizace

Aplikace DQM vyžaduje frontu pro použití s pořadovými čísly a logickými identifikátory pracovních jednotek (LUWID). Musíte se ujistit, že je fronta k dispozici s názvem SYSTEM.CHANNEL.SYNCQ (viz Plánování v z/OS). Tato fronta musí být k dispozici, jinak se iniciátor kanálu nemůže spustit.

Ujistěte se, že jste definovali tuto frontu pomocí INDXTYPE (MSGID). Tento atribut zlepšuje rychlost přístupu k nim.

Fronty příkazů kanálu

Musíte se ujistit, že pro váš systém existuje fronta příkazů kanálu s názvem SYSTEM.CHANNEL.INITQ.

Pokud inicializátor kanálu zjistí problém se SYSTEM SYSTEM.CHANNEL.INITQnemůže normálně pokračovat, dokud nebude problém opraven. Problém může být jeden z následujících:

- Fronta je plná
- Fronta není povolena pro vložení
- Sada stránek, na které se fronta nachází, je plná.
- Inicializátor kanálu nemá správnou autorizaci zabezpečení pro frontu.

Pokud je definice fronty změněna na GET (DISABLED), když je spuštěn inicializátor kanálu, iniciátor nemůže získat zprávy z fronty a ukončí se.

Spuštění inicializátoru kanálu

Spouštění je implementováno pomocí inicializátoru kanálu. V systému IBM MQ for z/OSje iniciátor spuštěn příkazem MQSC `START CHINIT`.

Zastavení inicializátoru kanálu

Inicializátor kanálu je při zastavení správce front automaticky zastaven. Potřebujete-li zastavit inicializátor kanálu, ale nikoli správce front, můžete použít příkaz MQSC `STOP CHINIT`.

z/OS Monitorování a řízení kanálů na systému z/OS

Pomocí panelů a příkazů DQM můžete vytvářet, monitorovat a řídit kanály pro vzdálené správce front.

Každý správce front z/OS má program DQM (*inicializátor kanálu*). pro řízení propojení se vzdálenými správci front pomocí nativních prostředků z/OS .

Implementace těchto panelů a příkazů v systému z/OS je integrována do provozních a řídicích panelů a příkazů MQSC. V organizaci těchto dvou sad panelů a příkazů se nerozlišuje.

Můžete také zadat příkazy pomocí příkazů PCF (Programmable Command Format). Informace o použití těchto příkazů naleznete v tématu Automatizace úloh administrace .

Informace v této části platí ve všech případech, kdy je iniciátor kanálu použit pro distribuované řazení do front. Použije se bez ohledu na to, zda používáte skupiny sdílení front nebo řazení do front v rámci skupiny.

Funkce řízení kanálu DQM

Přehled modelu distribuované správy front viz “Odesílání a příjem zpráv” na stránce 210.

Funkce řízení kanálu se skládá z panelů, příkazů a programů, dvou front synchronizace, front příkazů kanálu a definic kanálů. Toto téma obsahuje stručný popis komponent funkce řízení kanálu.

- Definice kanálů jsou uchovávány jako objekty v sadě stránek nula nebo v adresáři Db2, stejně jako ostatní objekty IBM MQ v souboru z/OS.
- Pomocí operací a ovládacích panelů, příkazů MQSC nebo příkazů PCF můžete:
  - Vytvoření, kopírování, zobrazení, změna a odstranění definic kanálů
  - Spuštění a zastavení inicializátorů a modulů listener kanálu
  - Spustit, zastavit a ping kanály, resetovat pořadová čísla kanálů a vyřešit neověřené zprávy, když nelze znovu navázat spojení.
  - Zobrazit informace o stavu kanálů
  - Zobrazení informací o aplikaci DQM

  K zadání příkazů MQSC můžete použít zejména vstupní datovou sadu inicializace CSQINPX. Tuto sadu lze zpracovat při každém spuštění inicializátoru kanálu. Další informace naleznete v tématu Příkazy inicializace.
- Existují dvě fronty (SYSTEM.CHANNEL.SYNCQ a SYSTEM.QSG.CHANNEL.SYNCQ) se používá pro účely opětovné synchronizace kanálu. Z důvodů výkonu definujte tyto fronty s hodnotou INDXTYPE (MSGID).
- Fronta příkazů kanálu (SYSTEM.CHANNEL.INITQ) se používá k uchování příkazů pro iniciátory kanálů, kanály a listenery.
- Program funkce řízení kanálu se spouští ve vlastním adresním prostoru, odděleně od správce front, a skládá se z inicializátoru kanálu, modulů listener, MCA, monitoru spouštěčů a obslužné rutiny příkazů.
- Informace o skupinách sdílení front a sdílených kanálech naleznete v tématu Sdílené fronty a skupiny sdílení front.
- Informace o řazení do front v rámci skupiny naleznete v tématu Řízení front v rámci skupiny .

Správa kanálů na webu z/OS

Informace o správě kanálů, inicializátorů kanálů a modulů listener získáte pomocí odkazů v následující tabulce:

Tabulka 64. Úlohy kanálu	
Úloha, která se má provést	**Příkaz MQSC**
Definovat kanál	Definovat kanál
Změnit definici kanálu	ALTER CHANNEL
Zobrazit definici kanálu	ZOBRAZIT KANÁL
Odstranit definici kanálu	Odstranit kanál
Spustit inicializátor kanálu	START CHINIT
Zastavit inicializátor kanálu	ZASTAVIT CHINIT
Zobrazit informace o inicializátoru kanálu	ZOBRAZIT CHINIT
Spustit modul listener kanálu	Spustit listener
Zastavit modul listener kanálu	Ukončit listener
Spuštění kanálu	Spustit kanál
Test kanálu	Odeslat signál Ping pro kanál
Resetovat pořadová čísla zpráv pro kanál	Resetovat kanál
Vyřešení nejistých zpráv v kanálu	Vyřešit kanál
Zastavit kanál	Ukončit kanál
Zobrazit stav kanálu	ZOBRAZIT STAV
Zobrazit kanály klastru	ZOBRAZIT MODUL CLUSQMGR

Související pojmy

“Použití panelů a příkazů” na stránce 956
Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo operace a ovládací panely.

“nastaveníIBM MQ for z/OS” na stránce 876
Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

“Nastavení komunikace pro z/OS” na stránce 970
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nezbytné, aby bylo připojení definováno a k dispozici. Tento oddíl vysvětluje, jak definovat připojení.

“Příprava produktu IBM MQ for z/OS pro aplikaci DQM se skupinami sdílení front” na stránce 975
Podle pokynů v této části můžete konfigurovat distribuované řazení do front se skupinami sdílení front v systému IBM MQ for z/OS.

“Nastavení komunikace pro produkt IBM MQ for z/OS pomocí skupin sdílení front” na stránce 979
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby bylo připojení definováno a k dispozici.

Související úlohy

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 950

Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

z/OS *Použití panelů a příkazů*

Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo operace a ovládací panely.

Informace o příkazech MQSC naleznete v tématu Administrace IBM MQ pomocí příkazů MQSC. Informace o příkazech PCF naleznete v tématu Automatizace administrace pomocí příkazů Programmable Command Formats.

Použití počátečního panelu

Úvod k vyvolání operací a ovládacích panelů pomocí funkčních kláves a získání nápovědy viz Administrace IBM MQ for z/OS.

Poznámka: Chcete-li používat operace a ovládací panely, musíte mít správnou autorizaci zabezpečení; další informace naleznete v tématu Administrace IBM MQ for z/OS a v dílčích tématech. Obrázek 106 na stránce 956 zobrazuje panel, který se zobrazí při spuštění relace panelu. Text za panelem vysvětluje akce, které jste provedli na tomto panelu.

```
IBM MQ for z/OS - Main Menu

Complete fields. Then press Enter.

Action . . . . . . . . . . 1   0. List with filter  4. Manage
1. List or Display  5. Perform
2. Define like    6. Start
3. Alter       7. Stop
8. Command
Object type . . . . . . . . CHANNEL    +
Name . . . . . . . . . . . . *
Disposition . . . . . . . . A Q=Qmgr, C=Copy, P=Private, G=Group,
S=Shared, A=All

Connect name . . . . . . . MQ25 - local queue manager or group
Target queue manager . . . MQ25
- connected or remote queue manager for command input
Action queue manager . . . MQ25 - command scope in group
Response wait time . . . . 10  5 - 999 seconds

(C) Copyright IBM Corporation 1993, 2024. All rights reserved.

Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Prompt  F9=SwapNext F10=Messages
F12=Cancel
```

Obrázek 106. Počáteční panel operací a ovládacích prvků

Z tohoto panelu můžete:

- Vyberte akci, kterou chcete provést, zadáním odpovídajícího čísla do pole **Akce** .
- Uveďte typ objektu, se kterým chcete pracovat. Stiskněte klávesu F4 , abyste získali seznam typů objektů, pokud si nejste jisti, jaké jsou.
- Zobrazí seznam objektů uvedeného typu. Zadejte hvězdičku (*) do pole **Název** a stiskněte klávesu Enter. Zobrazí se seznam objektů (uvedeného typu), které již byly v tomto subsystému definovány. Pak můžete vybrat jeden nebo více objektů, se kterými budete pracovat v posloupnosti. Obrázek 107 na stránce 957 zobrazuje seznam kanálů vytvořených tímto způsobem.
- Do pole **Odebrání** zadejte dispozice objektů, se kterými chcete pracovat, ve skupině sdílení front. Dispozice určuje, kde je objekt uchován a jak se objekt chová.
- V poli **Název připojení** vyberte lokálního správce front nebo skupinu sdílení front, ke které se chcete připojit. Chcete-li zadat příkazy pro vzdáleného správce front, vyberte buď pole **Cílový správce front** , nebo pole **Správce front akcí** v závislosti na tom, zda vzdálený správce front není nebo není členem skupiny sdílení front. Pokud vzdálený správce front není členem skupiny sdílení front, vyberte pole

Cílový správce front . Pokud je vzdálený správce front členem skupiny sdílení front, vyberte pole **Správce front akcí** .

- V poli **Doba čekání odezvy** zvolte dobu čekání na přijetí odpovědí.

```
List Channels - MQ25          Row 1 of 8

Type action codes, then press Enter. Press F11 to display connection status.
1=Display  2=Define like  3=Alter  4=Manage  5=Perform
6=Start   7=Stop

Name         Type     Disposition  Status
<> *           CHANNEL    ALL   MQ25
_  SYSTEM.DEF.CLNTCONN  CLNTCONN   QMGR  MQ25
_  SYSTEM.DEF.CLUSRCVR  CLUSRCVR   QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.CLUSSDR  CLUSSDR    QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.RECEIVER  RECEIVER   QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.REQUESTER REQUESTER   QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.SENDER   SENDER    QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.SERVER   SERVER    QMGR  MQ25 INACTIVE
_  SYSTEM.DEF.SVRCONN  SVRCONN    QMGR  MQ25 INACTIVE
******** End of list ********



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Filter  F5=Refresh  F7=Bkwd
F8=Fwd    F9=SwapNext F10=Messages F11=Status  F12=Cancel
```

Obrázek 107. Výpis kanálů

z/OS *Definování kanálu v systému z/OS*

V systému z/OSmůžete definovat kanál pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Procedura

- Chcete-li definovat kanál pomocí příkazů MQSC, použijte příkaz **DEFINE CHANNEL** .
- Chcete-li použít operace a ovládací panely počínaje počátečním panelem, vyplňte následující pole a stiskněte klávesu Enter:

Tabulka 65. Ovládací a ovládací panely: počáteční panelová pole

Pole	**Hodnota, která se má zadat do pole**
Akce	2 (Definovat jako)
Typ objektu	Typ kanálu (například SENDER) nebo CHANNEL
Název	
Dispozice	Umístění nového objektu.

Zobrazí se některé panely s informacemi o názvu a atributech, které chcete pro kanál, který definujete. Jsou inicializovány s výchozími hodnotami atributu. Změňte všechny požadované hodnoty před stisknutím klávesy Enter.

Poznámka: Pokud jste do pole **typ objektu** zadali hodnotu CHANNEL, zobrazí se nejprve panel **Vybrat platný typ kanálu** .

Chcete-li definovat kanál se stejnými atributy jako existující kanál, vložte název kanálu, který chcete zkopírovat, do pole **Name** na počátečním panelu. Panely jsou inicializovány s atributy existujícího objektu.

Informace o atributech kanálu naleznete v tématu Atributy kanálu.

Poznámka:

1. Pojmenujte všechny kanály ve vaší síti jedinečně. Jak ukazuje Diagram sítě zobrazující všechny kanály, včetně názvů zdrojového a cílového správce front v názvu kanálu je dobrým způsobem, jak toto pojmenování provést.

Jak pokračovat dále

Poté, co jste definovali svůj kanál, musíte zabezpečit svůj kanál. Další informace viz téma “Zabezpečení kanálu” na stránce 959.

z/OS *Změna definice kanálu*

Definici kanálu můžete změnit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li změnit definici kanálu pomocí příkazů MQSC, použijte příkaz ALTER CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	3 (změna)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.ALTER
Dispozice	Umístění uloženého objektu.

Zobrazí se některé panely obsahující informace o aktuálních atributech kanálu. Změňte libovolná nechráněná pole přepsáním nové hodnoty a pak stiskněte klávesu Enter pro změnu definice kanálu.

Informace o atributech kanálu naleznete v tématu Atributy kanálu.

z/OS *Zobrazení definice kanálu*

Definici kanálu můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zobrazit definici kanálu pomocí příkazů MQSC, použijte příkaz DISPLAY CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	1 (Seznam nebo zobrazení)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.DISPLAY
Dispozice	Umístění objektu.

Zobrazí se některé panely zobrazující informace o aktuálních atributech kanálu.

Informace o atributech kanálu naleznete v tématu Atributy kanálu.

z/OS *Odstranění definice kanálu*

Definici kanálu můžete odstranit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li odstranit definici kanálu pomocí příkazů MQSC, použijte příkaz DELETE CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	4 (Spravovat)

Pole	Hodnota
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.DELETE
Dispozice	Umístění objektu.

Zobrazí se vám další panel. Na tomto panelu vyberte typ funkce 1.

Stiskněte klávesu Enter pro odstranění definice kanálu; budete vyzváni k potvrzení, že chcete odstranit definici kanálu opětovným stisknutím klávesy Enter.

Poznámka: Inicializátor kanálu musí být spuštěn před odstraněním definice kanálu (s výjimkou kanálů připojení klienta).

z/OS *Zobrazení informací o inicializátoru kanálu*

Informace o inicializátoru kanálu můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zobrazit informace o inicializátoru kanálu pomocí příkazů MQSC, použijte příkaz DISPLAY CHINIT.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	1 (Zobrazení)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se vám další panel. Na tomto panelu vyberte typ funkce 1.

Poznámka:

1. Zobrazení informací o distribuovaných frontách může trvat delší dobu, pokud máte mnoho kanálů.
2. Inicializátor kanálu musí být spuštěn, aby bylo možné zobrazit informace o distribuovaném řazení do front.

z/OS *Zabezpečení kanálu*

Kanál můžete zabezpečit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zabezpečit kanál pomocí příkazů MQSC, použijte příkaz SET CHLAUTH.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	8

Zobrazí se vám editor, ve kterém můžete zadat příkaz MQSC, v tomto případě příkaz CHLAUTH, viz Obrázek 108 na stránce 960. Po dokončení zadávání příkazu jsou zapotřebí znaménka plus (+). Zadáním příkazu PF3 ukončete editor a odešlete příkaz na příkazový server.

```
****************************** Top of Data ******************************
000001 SET CHLAUTH(SYSTEM.DEF.SVRCONN) +
000002 TYPE(SSLPEERMAP) +
000003 SSLPEER('CN="John Smith"') +
000004 MCAUSER('PUBLIC')
****** **************************** Bottom of Data ****************************

Command ===>                          Scroll ===> PAGE
F1=Help   F3=Exit   F4=LineEdit F12=Cancel
```

Obrázek 108. Záznam příkazu

Výstup příkazu se vám pak zobrazí, viz Obrázek 109 na stránce 960 .

```
****** **************************** Top of Data ******************************
000001 CSQU000I CSQUTIL IBM MQ for z/OS V7.1.0
000002 CSQU001I CSQUTIL Queue Manager Utility - 2011-04-20 14:42:58
000003 COMMAND TGTQMGR(MQ23) RESPTIME(30)
000004 CSQU127I Executing COMMAND using input from CSQUCMD data set
000005 CSQU120I Connecting to MQ23
000006 CSQU121I Connected to queue manager MQ23
000007 CSQU055I Target queue manager is MQ23
000008 SET CHLAUTH(SYSTEM.DEF.SVRCONN) +
000009 TYPE(SSLPEERMAP) +
000010 SSLPEER('CN="John Smith"') +
000011 MCAUSER('PUBLIC')
000012 CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000000
000013 CSQ9022I !MQ23 CSQMSCA ' SET CHLAUTH' NORMAL COMPLETION
000014 CSQU057I 1 commands read
000015 CSQU058I 1 commands issued and responses received, 0 failed
000016 CSQU143I 1 COMMAND statements attempted
000017 CSQU144I 1 COMMAND statements executed successfully
000018 CSQU148I CSQUTIL Utility completed, return code=0
Command ===>                          Scroll ===> PAGE
F1=Help   F3=Exit   F5=Rfind   F6=Rchange  F9=SwapNext F12=Cancel
```

Obrázek 109. Výstup příkazu

z/OS *Spuštění inicializátoru kanálu*

Inicializátor kanálu můžete spustit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li spustit inicializátor kanálu pomocí příkazů MQSC, použijte příkaz START CHINIT.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	6 (Začátek)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Spustit systémovou funkci. Text následující za následujícím panelem vysvětluje, jakou akci je třeba provést:

```
Start a System Function

Select function type, complete fields, then press Enter to start system
function.

Function type . . . . . _   1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
JCL substitution . . . . . _____________________________________________
_____________________________________________

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP
LU name (LU6.2) . . . . . _________________
Port number (TCP/IP) . . . 1414
IP address (TCP/IP) . . . _____________________________________________


Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 110. Spuštění systémové funkce

Vyberte typ funkce 1 (inicializátor kanálu) a stiskněte klávesu Enter.

z/OS *Zastavení inicializátoru kanálu*

Inicializátor kanálu můžete zastavit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zastavit inicializátor kanálu pomocí příkazů MQSC, použijte příkaz STOP CHINIT.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	7 (Zastavit)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Zastavit systémovou funkci. Text za panelem vysvětluje, jak používat tento panel:

```
Stop a System Function

Select function type, complete fields, then press Enter to stop system
function.

Function type . . . . . _   1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
Restart shared channels  Y Y=Yes, N=No

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP

Port number (TCP/IP) . . . _____
IP address (TCP/IP) . . . ________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 111. Zastavení ovládacího prvku funkce

Vyberte typ funkce 1 (inicializátor kanálu) a stiskněte klávesu Enter.

Inicializátor kanálu před zastavením čeká na zastavení všech spuštěných kanálů v klidovém režimu.

Poznámka: Pokud jsou některé kanály přijímacími nebo žadatelovými kanály, které jsou spuštěny, ale nejsou aktivní, požadavek na zastavení vydaný buď pro příjemce, nebo pro iniciátor odesílacího kanálu způsobí, že se okamžitě zastaví.

Pokud však zprávy proudí, iniciátor kanálu čeká na dokončení aktuální dávky zpráv, než se zastaví.

z/OS *Spuštění modulu listener kanálu*

Modul listener kanálu můžete spustit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li spustit modul listener kanálu pomocí příkazů MQSC, použijte příkaz START LISTENER.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	6 (Začátek)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Spustit systémovou funkci (viz Obrázek 110 na stránce 961).

Vyberte typ funkce 2 (modul listener kanálu). Vyberte příchozí dispozice. Vyberte typ přenosu. Je-li typ přenosu L, vyberte název LU. Je-li typ přenosu T, vyberte číslo portu a (volitelně) adresu IP. Stiskněte klávesu Enter.

Poznámka: Pro modul listener TCP/IP můžete spustit více kombinací portu a adresy IP.

z/OS *Zastavení modulu listener kanálu*

Modul listener kanálu můžete zastavit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zastavit modul listener kanálu pomocí příkazů MQSC, použijte příkaz STOP LISTENER.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	7 (Zastavit)
Typ objektu	SYSTÉM
Název	Prázdný

Zobrazí se panel Zastavit systémovou funkci (viz Obrázek 111 na stránce 962).

Vyberte typ funkce 2 (modul listener kanálu). Vyberte příchozí dispozice. Vyberte typ přenosu. Je-li typ přenosu 'T', vyberte číslo portu a (volitelně) adresu IP. Stiskněte klávesu Enter.

Poznámka: V případě modulu listener protokolu TCP/IP můžete zastavit určité kombinace portu a adresy IP nebo můžete zastavit všechny kombinace.

z/OS *Spuštění kanálu*

Kanál můžete spustit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li spustit kanál pomocí příkazů MQSC, použijte příkaz START CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	6 (Začátek)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Spustit kanál. Text následující za panelem vysvětluje, jak panel používat:

```
Start a Channel

Select disposition, then press Enter to start channel.


Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
S=Shared on MQ25
A=Shared on any queue manager









Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 112. Spuštění kanálu

Vyberte dispozici instance kanálu a správce front, v němž má být spuštěn.

Stisknutím klávesy Enter spusťte kanál.

z/OS *Spuštění sdíleného kanálu*

Chcete-li spustit sdílený kanál a ponechat jej na nominovaném inicializátoru kanálu, použijte dispozice = S (v příkazu START CHANNEL zadejte CHLDISP (FIXSHARED)).

V daném okamžiku může být spuštěna pouze jedna instance sdíleného kanálu. Pokus o spuštění druhé instance kanálu se nezdařil.

Při spuštění kanálu tímto způsobem platí pro tento kanál následující pravidla:

- Kanál můžete zastavit z libovolného správce front ve skupině sdílení front. Můžete jej zastavit i v případě, že inicializátor kanálu, na kterém byl spuštěn, není v době zadání požadavku na zastavení kanálu spuštěn. Po zastavení kanálu jej můžete restartovat zadáním dispozice = S (CHLDISP (FIXSHARED)) na stejném nebo jiném inicializátoru kanálu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Pokud je kanál ve stavu spuštění nebo opakování, můžete jej restartovat zadáním dispozice = S (CHLDISP (FIXSHARED)) na stejném nebo jiném inicializátoru kanálu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Kanál je způsobilý ke spuštění spouštěče, když přejde do neaktivního stavu. Sdílené kanály spouštěné spouštěčem mají vždy sdílenou dispozici (CHLDISP (SHARED)).
- Kanál je způsobilý ke spuštění s CHLDISP (FIXSHARED) na libovolném inicializátoru kanálu, když přejde do neaktivního stavu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Kanál není obnoven žádným jiným aktivním inicializátorem kanálu ve skupině sdílení front, když je inicializátor kanálu, na kterém byl spuštěn, zastaven pomocí příkazu SHARED (RESTART) nebo když je inicializátor kanálu nestandardně ukončen. Kanál je obnoven pouze v případě, že je inicializátor kanálu, na kterém byl spuštěn, znovu spuštěn. Dojde k zastavení nezdařených pokusů o zotavení kanálu, které jsou předány jiným inicializátorům kanálu ve skupině sdílení front, což by se přidalo k jejich pracovní zátěži.

z/OS *Testování kanálu*

Kanál můžete testovat pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li testovat kanál pomocí příkazů MQSC, použijte příkaz PING CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	5 (Provést)
Typ objektu	SENDER, SERVER nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu kanálu.

Zobrazí se panel Provést funkci kanálu. Text následující za panelem vysvětluje, jak panel používat:

```
Perform a Channel Function

Select function type, complete fields, then press Enter.


Function type . . . . . _   1. Reset  3. Resolve with commit
2. Ping  4. Resolve with backout

Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
S=Shared on MQ25
A=Shared on any queue manager

Sequence number for reset . . 1     1 - 999999999
Data length for ping . . . . 16   16 - 32768



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 113. Testování kanálu

Vyberte typ funkce 2 (ping).

Vyberte dispozici kanálu, pro který má být test proveden, a pro kterého správce front má být testován.

Délka dat je na začátku nastavena na 16. Změňte jej, pokud chcete, a stiskněte klávesu Enter.

z/OS *Resetování pořadových čísel zpráv pro kanál*

Pořadová čísla zpráv pro kanál můžete resetovat pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li pomocí příkazů MQSC resetovat pořadová čísla kanálu, použijte příkaz RESET CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	5 (Provést)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu kanálu.

Zobrazí se panel Provést funkci kanálu (viz Obrázek 113 na stránce 965).

Vyberte typ funkce 1 (reset).

Vyberte dispozici kanálu, pro který má být proveden reset a pro kterého má být proveden správce front.

Pole **Pořadové číslo** je na počátku nastaveno na hodnotu jedna. Změňte tuto hodnotu, pokud chcete, a stiskněte klávesu Enter.

z/OS *Řešení nejistých zpráv v kanálu*

Pochybné zprávy v kanálu můžete vyřešit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li vyřešit neověřené zprávy v kanálu pomocí příkazů MQSC, použijte volbu RESOLVE CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	5 (Provést)
Typ objektu	SENDER, SERVER nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Provést funkci kanálu (viz Obrázek 113 na stránce 965).

Vyberte typ funkce 3 nebo 4 (vyřešit s potvrzením nebo backout). (Další informace viz “Zpracování nejistých kanálů” na stránce 229 .)

Vyberte dispozice kanálu, pro který má být provedeno rozlišení, a správce front, pro kterého má být provedeno. Stiskněte klávesu Enter.

z/OS *Zastavení kanálu*

Kanál můžete zastavit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zastavit kanál pomocí příkazů MQSC, použijte příkaz STOP CHANNEL.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	7 (Zastavit)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Zastavit kanál. Text následující za panelem vysvětluje, jak panel používat:

```
Stop a Channel

Complete fields, then press Enter to stop channel.


Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
A=Shared on any queue manager

Stop mode . . . . . 1   1. Quiesce  2. Force
Stop status . . . . . 1   1. Stopped  2. Inactive

Queue manager . . . . . ________________________________________________
Connection name . . . . . ________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 114. Zastavení kanálu

Vyberte dispozici kanálu, pro který má být provedeno zastavení, a pro kterého má být zastaven správce front.

Zvolte požadovaný režim zastavení:

Uvést do klidového stavu
Kanál se zastaví po dokončení aktuální zprávy a poté se ukončí dávka, a to i v případě, že nebyla dosažena hodnota velikosti dávky a v přenosové frontě již čekají zprávy. Nejsou spuštěny žádné nové dávky. Tento režim je výchozí.

Vynutit
Kanál se okamžitě zastaví. Pokud probíhá zpracování dávky zpráv, může dojít k situaci, která je "nejistá".

Vyberte správce front a název připojení pro kanál, který chcete zastavit.

Zvolte požadovaný stav:

Zastaveno
Kanál není automaticky restartován a musí být restartován ručně. Tento režim je výchozí, pokud není zadán žádný správce front ani název připojení. Je-li uveden název, není povolen.

Neaktivní
Kanál se v případě potřeby automaticky restartuje. Tento režim je výchozí, pokud je zadán správce front nebo název připojení.

Chcete-li kanál zastavit, stiskněte klávesu Enter.

Další informace viz “Zastavení a uvedení kanálů do klidového stavu” na stránce 227. Informace o restartování zastavených kanálů viz “Restartování zastavených kanálů” na stránce 229.

Poznámka: Pokud se sdílený kanál nachází ve stavu opakování a iniciátor kanálu, na kterém byl spuštěn, není spuštěn, je požadavek STOP pro kanál zadán ve správci front, na kterém byl zadán příkaz.

z/OS *Zobrazení stavu kanálu*

Stav kanálu můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zobrazit stav kanálu nebo sady kanálů pomocí příkazů MQSC, použijte příkaz DISPLAY CHSTATUS.

Poznámka: Zobrazení informací o stavu kanálu může trvat delší dobu, pokud máte mnoho kanálů.

Pomocí operací a ovládacích panelů na panelu Seznam kanálů (viz Obrázek 107 na stránce 957) se pro každý kanál zobrazí následující souhrn stavu kanálů:

INACTIVE	Nejsou aktivní žádná připojení
stav	Jedno připojení je aktivní
nnn stav	Aktuální je více než jedno připojení a všechna aktuální připojení mají stejný stav.
nnn CURRENT	Aktuální je více než jedno připojení a aktuální připojení nemají stejný stav.
Prázdný	Produkt IBM MQ nemůže určit, kolik připojení je aktivních (například proto, že není spuštěn inicializátor kanálu). **Poznámka:** Pro objekty kanálu s dispozicí GROUP není zobrazen žádný stav.

kde *nnn* je počet aktivních připojení a *status* je jedna z následujících:

Inicializovat	INICIALIZACE
BIND	Vazba
SPUSTIT	SPOUŠTĚNÍ
RUN	RUNNING
ZASTAVIT	ZASTAVOVÁNÍ nebo ZASTAVENO
RETRY	Opakovaný pokus

REQST	Zpracování požadavků

Chcete-li zobrazit další informace o stavu kanálu, stiskněte klávesu Status (F11) na panelu Seznam kanálů nebo na panelu Zobrazit nebo změnit kanál, abyste zobrazili panel Seznam kanálů-Aktuální stav (viz Obrázek 115 na stránce 968).

```
List Channels - Current Status - MQ25      Row 1 of 16

Type action codes, then press Enter. Press F11 to display saved status.
1=Display current status

Channel name     Connection name                 State
Start time      Messages Last message time  Type   Disposition
<> *                          CHANNEL  ALL   MQ25

_ RMA0.CIRCUIT.ACL.F  RMA1                       STOP
_  2005-03-21 10.22.36 557735  2005-03-24 09.51.11 SENDER  PRIVATE MQ25
_ RMA0.CIRCUIT.ACL.N  RMA1
_  2005-03-21 10.23.09 378675  2005-03-24 09.51.10 SENDER  PRIVATE MQ25
_ RMA0.CIRCUIT.CL.F  RMA2
_  2005-03-24 01.12.51 45544   2005-03-24 09.51.08 SENDER  PRIVATE MQ25
_ RMA0.CIRCUIT.CL.N  RMA2
_  2005-03-24 01.13.55 45560   2005-03-24 09.51.11 SENDER  PRIVATE MQ25
_ RMA1.CIRCUIT.CL.F  RMA1
_  2005-03-21 10.24.12 360757  2005-03-24 09.51.11 RECEIVER PRIVATE MQ25
_ RMA1.CIRCUIT.CL.N  RMA1
_  2005-03-21 10.23.40 302870  2005-03-24 09.51.09 RECEIVER PRIVATE MQ25
******** End of list ********
Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Filter  F5=Refresh  F7=Bkwd
F8=Fwd    F9=SwapNext F10=Messages F11=Saved  F12=Cancel
```

Obrázek 115. Výpis připojení kanálu

Hodnoty pro stav jsou následující:

Inicializovat	INICIALIZACE
BIND	Vazba
SPUSTIT	SPOUŠTĚNÍ
RUN	RUNNING
ZASTAVIT	ZASTAVOVÁNÍ nebo ZASTAVENO
RETRY	Opakovaný pokus
REQST	Zpracování požadavků
ZDVOJNÁSOBENÍ	ZASTAVENO a INDOUBT (ANO)

Další informace viz “Stavy kanálů” na stránce 220.

Stisknutím klávesy F11 můžete zobrazit podobný seznam připojení kanálů s uloženým stavem; stisknutím klávesy F11 se vrátíte do aktuálního seznamu. Uložený stav se nepoužije, dokud nebude na kanálu přenesena alespoň jedna dávka zpráv.

Pomocí kódu akce 1 nebo lomítka (/) vyberte připojení a stiskněte klávesu Enter. Zobrazí se panely Zobrazit aktuální stav připojení kanálu.

z/OS *Zobrazení kanálů klastru*

Kanály klastru můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a ovládacích panelů.

Chcete-li zobrazit všechny kanály klastru, které byly definovány (explicitně nebo pomocí automatické definice), použijte příkaz MQSC, DISPLAY CLUSQMGR.

Pomocí operací a ovládacích panelů, počínaje od počátečního panelu, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	1 (Seznam nebo zobrazení)
Typ objektu	CLUSCHL
Název	*

Zobrazí se panel jako obrázek Obrázek 116 na stránce 969, ve kterém informace pro každý kanál klastru zabírají tři řádky a obsahují jeho názvy kanálů, klastrů a správců front. Pro odesílací kanály klastru se zobrazí celkový stav.

```
List Cluster queue manager Channels - MQ25    Row 1 of 9

Type action codes, then press Enter. Press F11 to display connection status.
1=Display  5=Perform  6=Start  7=Stop

Channel name     Connection name                State
Type     Cluster name                   Suspended
Cluster queue manager name            Disposition
<>   *                         -    MQ25
_ TO.MQ90.T      HURSLEY.MACH90.COM(1590)
_  CLUSRCVR   VJH01T                     N
_   MQ90                       -    MQ25
_ TO.MQ95.T      HURSLEY.MACH95.COM(1595)            RUN
_  CLUSSDRA   VJH01T                     N
_   MQ95                       -    MQ25
_ TO.MQ96.T      HURSLEY.MACH96.COM(1596)            RUN
_  CLUSSDRB   VJH01T                     N
_   MQ96                       -    MQ25
******** End of list ********


Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F4=Filter  F5=Refresh  F7=Bkwd
F8=Fwd    F9=SwapNext F10=Messages F11=Status  F12=Cancel
```

Obrázek 116. Výpis kanálů klastru

Chcete-li zobrazit úplné informace o jednom nebo více kanálech, zadejte kód akce 1 pro jejich jména a stiskněte klávesu Enter. Použijte kódy akcí 5, 6 nebo 7 k provedení funkcí (jako je příkaz ping, vyřešení a reset) a ke spuštění nebo zastavení kanálu klastru.

Chcete-li zobrazit další informace o stavu kanálu, stiskněte klávesu Status (F11).

z/OS *Příprava produktu IBM MQ for z/OS na použití prostředku produktu zEnterprise Data Compression Express*

Prostředek zEnterprise Data Compression (zEDC) Express je k dispozici pro určité modely počítačů se systémem IBM Z , počínaje systémem IBM zEC12 GA2, s minimální úrovní z/OS z/OS 2.1.

Další informace viz zEnterprise Komprese dat (zEDC) .

Požadavky

V případě operačního systému IBM z15 a novějšího byl prostředek zEnterprise Data Compression (zEDC) Express přesunut z volitelné funkce v zásuvce PCIe I/O hardwarového systému, aby byl na čipu jako integrovaný akcelerátor pro zEDC. Při této změně jsou předpoklady konfigurace aktualizovány a závisí na vašem hardwarovém systému.

IBM z15 nebo novější

Podle úrovně operačního systému z/OSpoužijte jednu z následujících oprav PTF:

- z/OS 2.4: UJ00636
- z/OS 2.3: UJ00635
- z/OS 2.2: UJ00638
- z/OS 2.1: UJ00639

Pro systémy z15 nebo novější neexistují žádné hardwarové požadavky. Řešení Integrated Accelerator for zEDC v těchto systémech poskytuje vestavěnou akceleraci dat, takže již není zapotřebí samostatný adaptér.

IBM zEC12 GA2 do IBM z14

Váš systém musí mít také následující požadavky:

- Adaptér zEDC Express ® instalovaný v zásuvkách PCIe I/O hardwarového systému.
- Schopnost softwaru zEDC (volitelná, placená funkce) musí být povolena ve členu knihovny parametrů IFAPRDxx.

Postup

IBM zEC12 GA2 do IBM z14

Ujistěte se, že ID uživatele inicializátoru kanálu má oprávnění READ k FPZ.ACCELERATOR.COMPRESSION v profilu RACF FACILITY CLASS nebo ekvivalent v externím správci zabezpečení (ESM), který používá váš podnik.

Upozornění: Nepožaduje se pro IBM z15 nebo novější.

IBM zEnterprise zEC12 GA2 nebo novější

Konfigurujte kanál s COMPMSG (ZLIBFAST) na konci odesílání i příjmu. Po nakonfigurování se komprese zlib používá ke kompresi a dekompresi zpráv procházejících kanálem.

Komprese se provádí v zEDC , když je velikost dat, která se mají komprimovat, nad minimální prahovou hodnotou. Prahová hodnota závisí na použitém hardwaru IBM z

- IBM zEC12 GA2 až IBM z14 má minimální prahovou hodnotu 4KB
- IBM z15 nebo novější má minimální prahovou hodnotu 1KB

Pro zprávy pod prahovou hodnotou se v softwaru provádí komprese nebo inflace.

z/OS Nastavení komunikace pro z/OS

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nezbytné, aby bylo připojení definováno a k dispozici. Tento oddíl vysvětluje, jak definovat připojení.

DQM je služba vzdáleného řízení front pro produkt IBM MQ. Poskytuje programy pro řízení kanálů pro správce front, který vytváří rozhraní pro komunikační spojení. Tyto odkazy jsou řízeny systémovým operátorem. Definice kanálů uchovávané správou distribuovaných front používají tato připojení.

Vyberte jednu ze dvou forem komunikačního protokolu, které lze použít pro z/OS:

- “Definování připojení TCP na systému z/OS” na stránce 971
- “Definování připojení LU6.2 pro z/OS pomocí APPC/MVS” na stránce 974

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Každá definice kanálu musí jako atribut přenosového protokolu (typ přenosu) určovat pouze jeden protokol. Správce front může ke komunikaci použít více než jeden protokol.

Může být také užitečné se podívat na Příklad konfigurace- IBM MQ for z/OS . Pokud používáte skupiny sdílení front, viz “Nastavení komunikace pro produkt IBM MQ for z/OS pomocí skupin sdílení front” na stránce 979.

Související pojmy

“Použití panelů a příkazů” na stránce 956
Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo operace a ovládací panely.

“nastaveníIBM MQ for z/OS” na stránce 876
Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

“Monitorování a řízení kanálů na systému z/OS” na stránce 954
Pomocí panelů a příkazů DQM můžete vytvářet, monitorovat a řídit kanály pro vzdálené správce front.

“Příprava produktu IBM MQ for z/OS pro aplikaci DQM se skupinami sdílení front” na stránce 975
Podle pokynů v této části můžete konfigurovat distribuované řazení do front se skupinami sdílení front v systému IBM MQ for z/OS.

“Nastavení komunikace pro produkt IBM MQ for z/OS pomocí skupin sdílení front” na stránce 979
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby bylo připojení definováno a k dispozici.

Související úlohy

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 950
Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

z/OS *Definování připojení TCP na systému z/OS*

Chcete-li definovat připojení TCP, existuje řada nastavení, která se mají konfigurovat.

Název adresního prostoru TCP musí být uveden v datové sadě parametrů systému TCP, *tcpip*.TCPIP.DATA. V datové sadě musí být zahrnut příkaz "TCPIPJOBNAME *TCPIP_proc*" .

Používáte-li bránu firewall, musíte nakonfigurovat připojení produktu `allow` z inicializátoru kanálu na adresy v kanálech a ze vzdálených připojení do správce front.

Obvykle definice brány firewall konfiguruje odesílající adresu IP a port na cílovou adresu IP a port:

- Obraz z/OS může mít více než jeden název hostitele a možná budete muset nakonfigurovat bránu firewall s více adresami hostitele jako zdrojovou adresou.

  K zobrazení těchto názvů a adres můžete použít příkaz NETSTAT HOME.
- Inicializátor kanálu může mít více modulů listener na různých portech, takže musíte tyto porty nakonfigurovat.
- Používáte-li sdílený port pro skupinu sdílení front, musíte konfigurovat také sdílený port.

Adresní prostor inicializátoru kanálu musí mít oprávnění ke čtení datové sady. Pro přístup k protokolu TCPIP.DATA v závislosti na produktu TCP/IP a rozhraní, které používáte:

- Proměnná prostředí, RESOLVER_CONFIG
- /etc/resolv.conf v systému souborů
- // Příkaz SYSTCPD DD
- // Příkaz SYSTCPDD DD
- *jobname/userid*.TCPIP.DATA

- SYS1.TCPPARMS(TCPDATA)
- *zapname*.TCPIP.DATA

Také musíte být opatrní, abyste správně zadali kvalifikátor vyšší úrovně pro TCP/IP.

Potřebujete vhodně nakonfigurovaný server DNS (Domain Name System), který je schopen překladu názvu na adresu IP a překladu adresy IP na název.

Poznámka: Některé změny konfigurace vyhodnocovacího modulu vyžadují recyklaci aplikací, které jej používají, například IBM MQ.

Další informace jsou uvedeny v následujících tématech:

- Základní systém TCP/IP
- z/OS UNIX System Services.

Každý kanál TCP při spuštění používá prostředky TCP; možná budete muset upravit následující parametry ve vašem PROFILE.TCPIP :

ACBPOOLSIZE
Přidat jeden pro každý spuštěný kanál TCP plus jeden

CCBPOOLSIZE
Přidejte jednu pro každý spuštěný kanál TCP plus jednu pro každý dispečer DQM a jednu pro každý dispečer DQM.

VELIKOST DATABANKA
Přidat dva na jeden spuštěný kanál TCP plus jeden

MAXFILEPROC
Řídí, kolik kanálů může každý dispečer v inicializátoru kanálu zpracovat.

Tento parametr je uveden ve členu BPXPRMxx SYSI.PARMLIB. Ujistěte se, že jste zadali dostatečně velkou hodnotu pro vaše potřeby.

Ve výchozím nastavení je iniciátor kanálu schopen vytvářet vazby pouze na adresy IP přidružené k zásobníku uvedenému v atributu správce front TCPNAME. Chcete-li povolit, aby inicializátor kanálu komunikoval pomocí dalších zásobníků TCP/IP v systému, změňte atribut správce front TCPSTACK na MULTIPLE.

MQ Adv. CD Na kanál zpráv, který používá protokol TCP/IP, lze poukázat na IBM Aspera faspio Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována na Red Hat nebo Ubuntu Linuxnebo Windows. Viz Definování Aspera gateway připojení na Linux nebo Windows.

Související pojmy
“Konec odesílání” na stránce 972
Na odesílajícím konci připojení TCP/IP existuje řada nastavení, která se mají konfigurovat.

“Příjem na TCP” na stránce 973
Na přijímacím konci připojení TCP/IP existuje řada nastavení, která se mají konfigurovat.

“Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému z/OS” na stránce 973
Při příjmu v protokolu TCP/IP je nastaven maximální počet nevyřízených požadavků na připojení. Tyto neprovedené požadavky lze považovat za *nevyřízené* požadavky čekající na port TCP/IP, aby mohl modul listener přijmout požadavek.

z/OS *Konec odesílání*
Na odesílajícím konci připojení TCP/IP existuje řada nastavení, která se mají konfigurovat.

Pole názvu připojení (CONNAME) v definici kanálu musí být nastaveno buď na název hostitele (například MVSHUR1), nebo na síťovou adresu TCP cíle. Síťová adresa TCP může být v tečkovém desítkovém formátu IPv4 (například 127.0.0.1) nebo IPv6 hexadecimálním formátu (například 2001:DB8:0:0:0:0:0:0). Pokud

je název připojení názvem hostitele, je pro převod názvu hostitele na adresu hostitele TCP vyžadován server názvů TCP. (Tento požadavek je funkcí TCP, nikoli IBM MQ.)

Na zahajovacím konci připojení (typ odesílatele, žadatele a kanálu serveru) je možné zadat volitelné číslo portu pro připojení, například:

Název připojení
192.0.2.0(1555)

V tomto případě se inicializační ukončení pokusí připojit k přijímajícímu programu, který naslouchá na portu 1555.

Poznámka: Není-li uvedeno volitelné číslo portu, použije se výchozí číslo portu 1414.

Inicializátor kanálu může použít libovolný zásobník TCP/IP, který je aktivní a dostupný. Při výchozím nastavení iniciátor kanálu sváže své odchozí kanály s výchozí adresou IP pro zásobník TCP/IP uvedený v atributu správce front TCPNAME. Chcete-li se připojit přes jiný zásobník, musíte zadat buď název hostitele, nebo adresu IP zásobníku v atributu LOCLADDR kanálu.

z/OS *Příjem na TCP*

Na přijímacím konci připojení TCP/IP existuje řada nastavení, která se mají konfigurovat.

Programy přijímacího kanálu jsou spouštěny v reakci na spouštěcí požadavek odesílajícího kanálu. Chcete-li tak učinit, je třeba spustit program modulu listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program modulu listener spustíte příkazem START LISTENER nebo pomocí operací a ovládacích panelů.

Standardně:

- Program TCP Listener používá port 1414 a naslouchá na všech adresách dostupných pro váš zásobník TCP.
- Moduly listener protokolu TCP/IP se mohou vázat pouze na adresy přidružené k zásobníku TCP/IP uvedenému v atributu správce front TCPNAME.

Chcete-li spustit moduly listener pro jiné adresy nebo všechny dostupné zásobníky TCP, nastavte atribut správce front TCPSTACK na hodnotu 'MULTIPLE'.

Zadáním IPADDR v příkazu START LISTENER můžete spustit program modulu listener protokolu TCP tak, aby naslouchal pouze na určité adrese nebo názvu hostitele. Další informace viz téma Moduly listener.

z/OS *Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému z/OS*

Při příjmu v protokolu TCP/IP je nastaven maximální počet nevyřízených požadavků na připojení. Tyto neprovedené požadavky lze považovat za *nevyřízené* požadavky čekající na port TCP/IP, aby mohl modul listener přijmout požadavek.

Výchozí hodnota nevyřízených požadavků modulu listener na systému z/OS je 10000. Pokud nevyřízené požadavky dosáhnou těchto hodnot, připojení TCP/IP je odmítnuto a kanál není schopen se spustit.

V případě kanálů MCA to má za následek, že kanál přejde do stavu OPAKOVAT a později se znovu pokusí o připojení.

V případě připojení klienta klient obdrží od MQCONN kód příčiny MQRC_Q_MGR_NOT_AVAILABLE a může připojení zopakovat později.

Související pojmy

“Použití volby nevyřízených požadavků modulu listener protokolu TCP v systému IBM MQ for Multiplatforms” na stránce 260

V protokolu TCP se s připojeními zachází jako s neúplnými, pokud mezi serverem a klientem nedojde k třícestnému navázání komunikace. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nevyřízené požadavky čekající na port TCP, aby mohl modul listener přijmout požadavek.

z/OS *Definování připojení LU6.2 pro z/OS pomocí APPC/MVS*

Chcete-li definovat připojení LU6.2 , existuje řada nastavení, která se mají konfigurovat.

Nastavení APPC/MVS

Každá instance inicializátoru kanálu musí mít jméno LU, kterou má používat pro APPC/MVS, v členu APPCPMxx systému SYS1.PARMLIB, jako v následujícím příkladu:

```
LUADD ACBNAME( luname ) NOSCHED TPDATA(CSQ.APPCTP)
```

luname je název logické jednotky, která se má použít. NOSCHED je povinný; TPDATA se nepoužívá. Pro člena ASCHPMxx nebo datovou sadu profilu APPC/MVS TP nejsou nutná žádná přidání.

Datová sada informací o straně musí být rozšířena, aby definovala připojení používaná aplikací DQM. Podrobnosti o tom, jak to provést pomocí obslužného programu APPC ATBSDFMU, naleznete v dodané ukázce CSQ4SIDE . Podrobnosti o hodnotách TPNAME, které se mají použít, naleznete v následující tabulce:

Tabulka 66. Nastavení v lokálním systému z/OS pro vzdálenou platformu správce front

Vzdálená platforma	**TPNAME**
z/OS nebo MVS	Stejné jako TPNAME v odpovídajících postranních informacích o vzdáleném správci front.
IBM i	Stejná hodnota jako porovnávací hodnota v záznamu směrování v systému IBM i .
Systémy AIX and Linux	Stejné jako TPNAME v odpovídajících postranních informacích o vzdáleném správci front.
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo v vyvolatelném transakčním programu, který byl definován pomocí TpSetup na systému Windows.

Máte-li ve stejném počítači více než jednoho správce front, ujistěte se, že jsou názvy TPname v definicích kanálu jedinečné.

V prostředí, kde správce front komunikuje pomocí APPC se správcem front na stejném nebo jiném systému z/OS , se ujistěte, že buď definice VTAM pro komunikační LU uvádí SECACPT (ALREADYV), nebo že existuje profil RACF APPCLU pro připojení mezi LU, který uvádí CONVSEC (ALREADYV).

Příkaz z/OS VARY ACTIVE musí být vydán pro základní jednotku i jednotku LU modulu listener, než se pokusíte spustit příchozí nebo odchozí komunikaci.

Upozornění: Kromě nastavení APPC musíte zadat následující příkaz:

```
ALTER QMGR LUNAME(luname)
```

a restartujte inicializátor kanálu.

Další informace viz LUNAME .

Související pojmy

“Připojení k LU 6.2” na stránce 974
Chcete-li se připojit k jednotce LU 6.2, je třeba konfigurovat několik nastavení.

“Příjem na LU 6.2” na stránce 975
Chcete-li přijímat na jednotce LU 6.2, existuje řada nastavení, která je třeba konfigurovat.

z/OS *Připojení k LU 6.2*

Chcete-li se připojit k jednotce LU 6.2, je třeba konfigurovat několik nastavení.

Pole názvu připojení (CONNAME) v definici kanálu musí být nastaveno na symbolický název místa určení, jak je uvedeno v datové sadě informací o připojení pro APPC/MVS.

Název LU, který má být použit (definovaný pro APPC/MVS, jak je popsáno výše), musí být také uveden v parametrech inicializátoru kanálu. Musí být nastavena na stejnou logickou jednotku, která je používána pro příjem modulem listener.

Inicializátor kanálu používá volbu "SECURITY (SAME)" APPC/MVS, takže je to ID uživatele adresního prostoru inicializátoru kanálu, který se používá pro odchozí přenosy a je prezentován příjemci.

z/OS *Příjem na LU 6.2*

Chcete-li přijímat na jednotce LU 6.2, existuje řada nastavení, která je třeba konfigurovat.

Přijímající MCA jsou spouštěny jako odpověď na požadavek na spuštění z odesílajícího kanálu. Chcete-li tak učinit, je třeba spustit program modulu listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Program modulu listener je server APPC/MVS. Spustíte jej pomocí příkazu START LISTENER nebo pomocí operací a ovládacích panelů. Je třeba určit jméno LU, které má být použito se symbolickým názvem místa určení definovaným v datové sadě s informacemi o straně. Takto identifikovaná lokální LU musí být stejná jako ta, která se používá pro odchozí přenosy, jak je nastaveno v parametrech inicializátoru kanálu.

z/OS Příprava produktu IBM MQ for z/OS pro aplikaci DQM se skupinami sdílení front

Podle pokynů v této části můžete konfigurovat distribuované řazení do front se skupinami sdílení front v systému IBM MQ for z/OS.

Příklad konfigurace používající skupiny sdílení front naleznete v tématu Příklad konfigurace- IBM MQ for z/OS použití skupin sdílení front. Příklad plánování kanálu zpráv s použitím skupin sdílení front naleznete v tématu Příklad plánování kanálu zpráv pro z/OS použití skupin sdílení front.

Chcete-li povolit distribuované řazení do front se skupinami sdílení front, musíte vytvořit a nakonfigurovat následující komponenty:

- LU 6.2 a listenery TCP/IP
- Přenosové fronty a spouštění
- Agenti kanálů zpráv
- Fronta synchronizace

Po vytvoření komponent, které potřebujete k nastavení komunikace, viz “Nastavení komunikace pro produkt IBM MQ for z/OS pomocí skupin sdílení front” na stránce 979.

Informace o způsobu monitorování a řízení kanálů při použití skupin sdílení front naleznete v části “Monitorování a řízení kanálů na systému z/OS” na stránce 954.

V následujících oddílech naleznete informace o koncepcích a výhodách skupiny sdílení front.

Provozní třída

Sdílená fronta je typ lokální fronty, která nabízí jinou provozní třídu. Zprávy ve sdílené frontě jsou uloženy v prostředku CF (coupling facility), který umožňuje přístup ke všem správcům front ve skupině sdílení front. Zpráva ve sdílené frontě musí mít délku nejvýše 100 MB.

Generické rozhraní

Skupina sdílení front má generické rozhraní, které umožňuje síti zobrazit skupinu jako jedinou entitu. Tohoto pohledu je dosaženo použitím jediné generické adresy, kterou lze použít pro připojení k libovolnému správci front v rámci skupiny.

Každý správce front ve skupině sdílení front naslouchá příchozím požadavkům relace na adrese, která logicky souvisí s generickou adresou. Další informace viz “Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front” na stránce 977.

Spuštění kanálu s vyrovnanou zátěží

Sdílená přenosová fronta může být obsluhována odchozím kanálem spuštěným na libovolném inicializátoru kanálu ve skupině sdílení front. Spuštění kanálu s vyrovnanou zátěží určuje, kam má směřovat příkaz spuštění kanálu. Je zvolen odpovídající inicializátor kanálu, který má přístup k nezbytnému komunikačnímu subsystému. Například kanál definovaný s TRPTYPE (LU6.2) nelze spustit na inicializátoru kanálu, který má přístup pouze k subsystému TCP/IP.

Volba inicializátoru kanálu závisí na zatížení kanálu a na prostoru iniciátoru kanálu. Zátěž kanálu je počet aktivních kanálů vyjádřený jako procentní část maximálního počtu aktivních kanálů povolených v parametrech inicializátoru kanálu. Světlá výška je rozdíl mezi počtem aktivních kanálů a maximálním povoleným počtem.

Příchozí sdílené kanály lze vyrovnávat zátěž v rámci skupiny sdílení front pomocí generické adresy, jak je popsáno v tématu “Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front” na stránce 977.

Obnova sdíleného kanálu

V následující tabulce jsou uvedeny typy selhání sdíleného kanálu a způsob zpracování jednotlivých typů.

Typ selhání:	**Co se stane:**
Selhání komunikačního subsystému inicializátoru kanálu	Kanály závislé na subsystému komunikace zadávají nový pokus kanálu a jsou restartovány v příslušném inicializátoru kanálu skupiny sdílení front pomocí příkazu pro spuštění s vyrovnanou zátěží.
Selhání inicializátoru kanálu	Iniciátor kanálu selže, ale přidružený správce front zůstane aktivní. Správce front monitoruje selhání a zahájí zpracování zotavení.
Selhání správce front	Správce front selže (selhání přidruženého inicializátoru kanálu). Ostatní správci front ve skupině sdílení front monitorují událost a zahajují zotavení typu peer.
Selhání sdíleného stavu	Informace o stavu kanálu jsou uloženy v adresáři Db2, takže při změně stavu kanálu dojde k selhání ztráty konektivity k produktu Db2 . Spuštěné kanály mohou pokračovat ve spuštění bez přístupu k těmto prostředkům. Při nezdařeném přístupu k produktu Db2kanál zadá nový pokus.

Zpracování obnovy sdíleného kanálu jménem systému, který selhal, vyžaduje, aby byla v systému spravujícím obnovu k načtení stavu sdíleného kanálu k dispozici konektivita k produktu Db2 .

Kanály klienta

Kanály připojení klienta mohou těžit z vysoké dostupnosti zpráv ve skupinách sdílení front, které jsou připojeny ke generickému rozhraní, namísto připojení ke specifickému správci front. Další informace naleznete v tématu Kanály připojení klienta.

Související pojmy

Sdílené fronty a skupiny sdílení front

“nastaveníIBM MQ for z/OS” na stránce 876
Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

“Klastry a skupiny sdílení front” na stránce 979
Sdílenou frontu můžete zpřístupnit pro klastr v jedné definici. Chcete-li tak učinit, zadejte název klastru při definování sdílené fronty.

“Kanály a serializace” na stránce 979

Během obnovy typu peer sdílené fronty agenti kanálu zpráv, kteří zpracovávají zprávy ve sdílených frontách, serializují svůj přístup k frontám.

Použití front v rámci skupiny

Související úlohy

“Konfigurace distribuovaných front” na stránce 189
Tento oddíl poskytuje podrobnější informace o interkomunikaci mezi instalacemi produktu IBM MQ , včetně definic front, definic kanálů, spouštění a procedur synchronizačních bodů.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 950
Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

z/OS *Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front*

Skupinové LU 6.2 a moduly listener protokolu TCP/IP naslouchají na adrese, která je logicky připojena ke generické adrese.

Pro modul listener LU 6.2 je určená skupina LUGROUP mapována na generický prostředek VTAM přidružený ke skupině sdílení front. Příklad nastavení této technologie viz “Definování připojení LU6.2 pro z/OS pomocí APPC/MVS” na stránce 974.

Pro modul listener TCP/IP může být určený port připojen ke generické adrese jedním z následujících způsobů:

- U front-endového směrovače, jako je například IBM Network Dispatcher, jsou příchozí požadavky na připojení předávány ze směrovače členům skupiny sdílení front.
- V případě distributoru prostředí sysplex TCP/IP je každému modulu listener, který je spuštěn a naslouchá na konkrétní adrese, která je nastavena jako distribuovaná DVIPA, přidělena část příchozích požadavků. Příklad nastavení této technologie viz Použití distributoru prostředí sysplex

z/OS *Přenosové fronty a spouštění pro skupiny sdílení front*

Sdílená přenosová fronta se používá k ukládání zpráv před jejich přesunutím ze skupiny sdílení front do cíle.

Jedná se o sdílenou frontu, která je přístupná všem správcům front ve skupině sdílení front.

Spouątění

Spuštěná sdílená fronta může generovat více než jednu zprávu spouštěče pro splněnou podmínku spouštěče. Pro každou lokální inicializační frontu definovanou ve správci front ve skupině sdílení front přidružené ke spuštěné sdílené frontě je vygenerována jedna zpráva spouštěče.

V případě distribuovaného řazení do front obdrží každý iniciátor kanálu zprávu spouštěče pro splněnou podmínku spouštěče sdílené přenosové fronty. Avšak pouze jeden inicializátor kanálu skutečně zpracuje spuštěné spuštění a ostatní bezpečně selžou. Spuštěný kanál se pak spustí se spuštěním s vyrovnanou zátěží (viz “Příprava produktu IBM MQ for z/OS pro aplikaci DQM se skupinami sdílení front” na stránce 975). který je spuštěn pro spuštění kanálu `QSG.TO.QM2`. Chcete-li vytvořit sdílenou přenosovou frontu, použijte příkazy IBM MQ (MQSC), jak ukazuje následující příklad:

```
DEFINE QLOCAL(QM2) DESCR('Transmission queue to QM2') +
USAGE(XMITQ) QSGDISP(SHARED) +
CFSTRUCT(APPLICATION1) INITQ(SYSTEM.CHANNEL.INITQ) +
TRIGGER TRIGDATA(QSG.TO.QM2)
```

Poznámka: Je-li pro spuštění nastavena sdílená fronta a připojení k prostředku Coupling Facility, který je hostitelem sdílené fronty, je ztraceno, může být vygenerována událost spouštěče a do inicializační fronty vložena zpráva. K tomu může dojít i v případě, že do původního nastavení sdílené fronty nebyla vložena žádná zpráva pro spuštění. To je způsobeno nadměrnou indikací bitů makrem IXLVECTR, jak je uvedeno v části Vektor oznámení seznamu.

z/OS *Agenti kanálu zpráv pro skupiny sdílení front*

Kanál lze spustit na inicializátoru kanálu pouze v případě, že má přístup k definici kanálu pro kanál s tímto názvem.

Agent kanálu zpráv je program IBM MQ , který řídí odesílání a příjem zpráv. Agenti kanálu zpráv přesouvají zprávy z jednoho správce front do jiného. Na každém konci kanálu je jeden agent kanálu zpráv.

Definice kanálu může být definována jako soukromá pro správce front nebo může být uložena ve sdíleném úložišti a k dispozici kdekoli (definice skupiny). To znamená, že kanál definovaný skupinou je k dispozici na libovolném inicializátoru kanálu ve skupině sdílení front.

Poznámka: Soukromou kopii definice skupiny lze změnit nebo odstranit.

Chcete-li vytvořit definice kanálů skupiny, použijte příkazy IBM MQ (MQSC), jak je uvedeno v následujících příkladech:

```
DEFINE CHL(QSG.TO.QM2) CHLTYPE(SDR) +
TRPTYPE(TCP) CONNAME(QM2.MACH.IBM.COM) +
XMITQ(QM2) QSGDISP(GROUP)
```

```
DEFINE CHL(QM2.TO.QSG) CHLTYPE(RCVR) TRPTYPE(TCP) +
QSGDISP(GROUP)
```

Existují dvě perspektivy, z nichž lze zobrazit agenty kanálů zpráv používané pro distribuované řazení do front se skupinami sdílení front:

Příchozí

Příchozí kanál je sdílený kanál, pokud je připojen ke správci front prostřednictvím modulu listener skupiny. Je připojen buď prostřednictvím generického rozhraní ke skupině sdílení front, poté přesměrován na správce front v rámci skupiny, nebo cílen na port skupiny specifického správce front nebo na název uzlu používaný modulem listener skupiny.

Odchozí

Odchozí kanál je sdílený kanál, pokud přesouvá zprávy ze sdílené přenosové fronty. V příkladových příkazech je odesílací kanál `QSG.TO.QM2` sdíleným kanálem, protože jeho přenosová fronta QM2 je definována s QSGDISP (SHARED).

z/OS *Fronta synchronizace pro skupiny sdílení front*

Sdílené kanály mají vlastní sdílenou frontu synchronizace s názvem SYSTEM.QSG.CHANNEL.SYNCQ.

Tato synchronizační fronta je přístupná pro libovolného člena skupiny sdílení front. (Soukromé kanály nadále používají soukromou frontu synchronizace. Viz “Definování objektů IBM MQ na z/OS” na stránce 953). To znamená, že kanál lze restartovat v jiné instanci správce front a inicializátoru kanálu v rámci skupiny sdílení front v případě selhání subsystému komunikací, inicializátoru kanálu nebo správce front. Další informace uvádí téma “Příprava produktu IBM MQ for z/OS pro aplikaci DQM se skupinami sdílení front” na stránce 975.

Správce DQM se skupinami sdílení front vyžaduje, aby byla sdílená fronta k dispozici s názvem SYSTEM.QSG.CHANNEL.SYNCQ. Tato fronta musí být k dispozici, aby mohl být modul listener skupiny úspěšně spuštěn.

Pokud modul listener skupiny selže, protože fronta nebyla k dispozici, lze frontu definovat a modul listener lze restartovat bez recyklování inicializátoru kanálu. Nesdílené kanály nejsou ovlivněny.

Ujistěte se, že jste definovali tuto frontu pomocí INDXTYPE (MSGID). Tato definice zvyšuje rychlost přístupu ke zprávám ve frontě.

z/OS *Klastry a skupiny sdílení front*

Sdílenou frontu můžete zpřístupnit pro klastr v jedné definici. Chcete-li tak učinit, zadejte název klastru při definování sdílené fronty.

Uživatelé v síti vidí sdílenou frontu jako hostovanou jednotlivými správci front v rámci skupiny sdílení front. (Sdílená fronta není ohlášena jako hostovaná skupinou sdílení front). Klienti mohou spouštět relace se všemi členy skupiny sdílení front a vkládat zprávy do stejné sdílené fronty.

Další informace viz téma “Konfigurace klastru správců front” na stránce 284.

z/OS *Kanály a serializace*

Během obnovy typu peer sdílené fronty agenti kanálu zpráv, kteří zpracovávají zprávy ve sdílených frontách, serializují svůj přístup k frontám.

Pokud dojde k selhání správce front ve skupině sdílení front v době, kdy agent kanálu zpráv pracuje s nepotvrzenými zprávami v jedné nebo více sdílených frontách, kanál a přidružený iniciátor kanálu budou ukončeny a pro správce front bude provedeno zotavení typu peer sdílené fronty.

Vzhledem k tomu, že zotavení typu peer pro sdílenou frontu je asynchronní aktivita, může se před dokončením zotavení typu peer pro sdílenou frontu pokusit o současné restartování kanálu v jiné části skupiny sdílení front. Dojde-li k této události, potvrzené zprávy mohou být zpracovány před zprávami, které jsou stále obnovovány. Aby se zajistilo, že zprávy nebudou tímto způsobem zpracovány mimo pořadí, agenti kanálu zpráv, kteří zpracovávají zprávy ve sdílených frontách, serializují svůj přístup k těmto frontám.

Pokus o spuštění kanálu, pro který stále probíhá zotavení typu peer sdílené fronty, může vést k selhání. Je vydána chybová zpráva informující o probíhajícím zotavení a kanál je uveden do stavu opakování. Po dokončení zotavení typu peer správce front může být kanál restartován v době dalšího opakování.

Pokus o RESOLVE, PING nebo DELETE kanálu může selhat ze stejné příčiny.

z/OS *Nastavení komunikace pro produkt IBM MQ for z/OS pomocí skupin sdílení front*

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby bylo připojení definováno a k dispozici.

Vyberte jednu ze dvou forem komunikačního protokolu, které lze použít:

- TCP
- LU 6.2 prostřednictvím APPC/MVS

Může být užitečné odkazovat se na Příklad konfigurace- IBM MQ for z/OS použití skupin sdílení front.

z/OS *Definování připojení TCP pro skupiny sdílení front*

Chcete-li definovat připojení TCP pro skupinu sdílení front, musí být nakonfigurovány určité atributy na odesílacím a přijímacím konci.

Informace o nastavení protokolu TCP viz “Definování připojení TCP na systému z/OS” na stránce 971.

Konec odesílání

Pole názvu připojení (CONNAME) v definici kanálu pro připojení ke skupině sdílení front musí být nastaveno na generické rozhraní vaší skupiny sdílení front (viz Skupiny sdílení front). Další podrobnosti viz Použití distributoru prostředí sysplex.

Příjem na TCP pomocí skupiny sdílení front

Programy pro příjem sdílených kanálů jsou spouštěny na základě požadavku na spuštění odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn modul listener, který zjišťuje příchozí síťové požadavky a spouští přidružený kanál. Tento program modulu listener spustíte příkazem START LISTENER, pomocí příchozího odebrání skupiny nebo pomocí operací a ovládacích panelů.

Všechny skupinové moduly listener ve skupině sdílení front musí naslouchat na stejném portu. Máte-li na jednom obrazu MVS spuštěn více než jeden inicializátor kanálu, můžete definovat virtuální adresy IP a spustit program modulu listener TCP tak, aby naslouchal pouze na určité adrese nebo názvu hostitele, a to zadáním IPADDR v příkazu START LISTENER. (Další informace viz START LISTENER.)

z/OS *Definování připojení LU 6.2 na systému z/OS*

Chcete-li definovat připojení LU 6.2 pro skupinu sdílení front, musí být nakonfigurovány určité atributy na odesílajícím a přijímajícím konci.

Informace o nastavení APPC/MVS naleznete v tématu Nastavení komunikace pro produkt z/OS .

Připojení k APPC/MVS (LU 6.2)

Pole názvu připojení (CONNAME) v definici kanálu pro připojení ke skupině sdílení front musí být nastaveno na symbolický název místa určení, jak je uvedeno v datové sadě informací o připojení pro APPC/MVS. Partnerská LU určená v tomto symbolickém místě určení musí být generickým názvem prostředku. Další podrobnosti viz Definování sebe v síti pomocí generických prostředků.

Příjem na LU 6.2 pomocí generického rozhraní

Příjem sdílených MCA se spouští v reakci na požadavek na spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn program skupinového modulu listener, který zjišťuje příchozí síťové požadavky a spouští přidružený kanál. Program modulu listener je server APPC/MVS. Spustíte jej pomocí příkazu START LISTENER, pomocí příchozí dispoziční skupiny nebo pomocí operací a ovládacích panelů. Chcete-li použít symbolické cílové jméno definované v datové sadě informací o straně, musíte zadat jméno LU. Další podrobnosti viz Definování sebe v síti pomocí generických prostředků.

z/OS Použití IBM MQ s IMS

Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

Chcete-li nakonfigurovat produkt IBM MQ a produkt IMS tak, aby spolupracovaly, musíte provést následující úlohy:

- “Nastavení adaptéru IMS” na stránce 981
- “Nastavení mostu IMS” na stránce 987

Související pojmy

IBM MQ a IMS

“Použití IBM MQ s CICS” na stránce 988

Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér IBM MQ CICS a volitelně komponenty produktu IBM MQ CICS bridge .

“Použití uživatelských procedur OTMA v adresáři IMS” na stránce 991

Toto téma použijte, chcete-li použít uživatelské procedury IMS Open Transaction Manager Access s produktem IBM MQ for z/OS.

IMS a IMS přemostění aplikací na IBM MQ for z/OS

Související úlohy

“Konfigurace správců front v systému z/OS” na stránce 871

Pomocí těchto pokynů můžete konfigurovat správce front v systému IBM MQ for z/OS.

Související odkazy

“Upgrade a použití služby v prostředí Language Environment nebo z/OS Callable Services” na stránce 988

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a podle vaší verze SMP/E.

z/OS Nastavení adaptéru IMS

Použití IBM MQ v rámci produktu IMS vyžaduje adaptér IBM MQ - IMS (obecně označovaný jako adaptér IMS).

Toto téma popisuje, jak zpřístupnit adaptér IMS pro subsystém IMS . Pokud nejste obeznámeni s přizpůsobením subsystému IMS , prohlédněte si IMS dokumentaci .

Chcete-li zpřístupnit adaptér IMS pro aplikace IMS , postupujte takto:

1. Definujte IBM MQ to IMS jako externí subsystém pomocí prostředku připojení externího subsystému IMS (ESAF).

   Viz “Definování IBM MQ do IMS” na stránce 982.
2. Zahrňte IBM MQ zaváděcí knihovnu thlqual.SCSQAUTH do zřetězení JOBLIB nebo STEPLIB v JCL pro řídicí oblast IMS a pro závislou oblast, která se připojuje k IBM MQ (pokud není v LPA nebo seznamu odkazů). Pokud nemáte oprávnění JOBLIB nebo STEPLIB, zahrňte jej také do zřetězení DFSESL po knihovně obsahující moduly IMS (obvykle IMS RESLIB).

   Dále uveďte thlqual.SCSQANLx (kde x je písmeno jazyka).

   Pokud je přítomen DFSESL, pak musí být SCSQAUTH a SCSQANLx zahrnuty do zřetězení nebo přidány do LNKLIST. Přidání do zřetězení STEPLIB nebo JOBLIB v JCL není dostatečné.
3. Zkopírujte program assembleru IBM MQ CSQQDEFV z thlqual.SCSQASMS do uživatelské knihovny.
4. Dodaný program CSQQDEFV obsahuje jeden název subsystému CSQ1 identifikovaný jako výchozí s tokenem jazykového rozhraní IMS (LIT) MQM1. Tento název můžete uchovat pro testování a ověření instalace.

   V případě produkčních subsystémů změňte název NAME=CSQ1 na svůj vlastní název subsystému, nebo použijte CSQ1. Podle potřeby můžete přidat další definice subsystému. Další informace o LIT viz “Definování správců front IBM MQ pro adaptér IMS” na stránce 985 .
5. Sestavte a propojte-upravte program tak, aby produkoval zaváděcí modul CSQQDEFV. Pro sestavení zahrňte knihovnu thlqual.SCSQMACS do zřetězení SYSLIB; použijte parametr linkování RENT. To se zobrazí v ukázkovém JCL v thlqual.SCSQPROC(CSQ4DEFV).
6. Zahrňte uživatelskou knihovnu obsahující modul CSQQDEFV, který jste vytvořili ve zřetězení JOBLIB nebo STEPLIB v JCL pro všechny závislé oblasti, které se připojují k IBM MQ. Umístěte tuto knihovnu před SCSQAUTH, protože SCSQAUTH má předvolený zaváděcí modul. Pokud tak neučiníte, obdržíte uživatele 3041 abend od IMS.
7. Pokud adaptér IMS zjistí neočekávanou chybu IBM MQ , vydá výpis paměti z/OS SNAP pro název definice dat CSQSNAP a vydá aplikaci kód příčiny MQRC_UNEXPECTED_ERROR. Pokud příkaz CSQSNAP DD nebyl v JCL závislé oblasti IMS , nebude proveden žádný výpis paměti. Pokud k tomu dojde, můžete do JCL zahrnout příkaz CSQSNAP DD a znovu spustit aplikaci. Vzhledem k tomu, že některé problémy mohou být občasné, doporučuje se zahrnout příkaz CSQSNAP DD pro zachycení příčiny selhání v době, kdy k nim dojde.
8. Chcete-li použít dynamická volání IBM MQ (popsaná v tématu Dynamické volání IBM MQ stubu), sestavte dynamický stub, jak ukazuje Obrázek 117 na stránce 982.
9. Chcete-li použít monitor spouštěčů IMS , definujte aplikaci CSQQTRMN monitoru spouštěčů IMS a proveďte PSBGEN a ACBGEN. Viz téma “Nastavení monitoru spouštěčů IMS” na stránce 986.
10. Používáte-li produkt RACF k ochraně prostředků ve třídě OPERCMDS, ujistěte se, že ID uživatele přidružené k adresnímu prostoru správce front IBM MQ má oprávnění k zadání příkazu MODIFY pro libovolný systém IMS , ke kterému se může připojit.

```
//DYNSTUB EXEC PGM=IEWL,PARM='RENT,REUS,MAP,XREF'
//SYSPRINT DD  SYSOUT=*
//ACSQMOD  DD  DISP=SHR,DSN=thlqual.SCSQLOAD
//IMSLIB   DD  DISP=SHR,DSN=ims.reslib
//SYSLMOD  DD  DISP=SHR,DSN=private.load[1]
//SYSUT1   DD  UNIT=SYSDA,SPACE=(CYL,1)
//SYSLIN   DD  *
  INCLUDE ACSQMOD(CSQQSTUB)
  INCLUDE IMSLIB(DFSLI000)
  ALIAS MQCONN,MQCONNX,MQDISC             MQI entry points
  ALIAS MQGET,MQPUT,MQPUT1                MQI entry points
  ALIAS MQOPEN,MQCLOSE                    MQI entry points
  ALIAS MQBACK,MQCMIT                     MQI entry points
  ALIAS CSQBBAK,CSQBCMT                   MQI entry points
  ALIAS MQINQ,MQSET                       MQI entry points
  ALIAS DFSPLI,PLITDLI                    IMS entry points
  ALIAS DFSCOBOL,CBLTDLI                  IMS entry points
  ALIAS DFSFOR,FORTDLI                    IMS entry points
  ALIAS DFSASM,ASMTDLI                    IMS entry points
  ALIAS DFSPASCL,PASTDLI                  IMS entry points
  ALIAS DFHEI01,DFHEI1                    IMS entry points
  ALIAS DFSAIBLI,AIBTDLI                  IMS entry points
  ALIAS DFSESS,DSNWLI,DSNHLI              IMS entry points
  ALIAS MQCRTMH,MQDLTMH,MQDLTMP           IMS entry points
  ALIAS MQINQMP,MQSETMP,MQMHBUF,MQBUFMH   IMS entry points
  MODE AMODE(31),RMODE(24)                Note RMODE setting
  NAME CSQQDYNS(R)
/*

[1]Specify the name of a library accessible to IMS applications that
want to make dynamic calls to IBM MQ.
```

Obrázek 117. Ukázka JCL pro odkazování-úprava stubu dynamického volání

Související pojmy

IBM MQ a IMS

“Nastavení mostu IMS” na stránce 987

Most IBM MQ - IMS je volitelná komponenta, která umožňuje produktu IBM MQ vstup a výstup do a z existujících programů a transakcí, které nejsou IBM MQpovoleny.

IMS a IMS přemostění aplikací na IBM MQ for z/OS

z/OS *Definování IBM MQ do IMS*

Parametr IBM MQ musí být definován pro řídicí oblast IMS a pro každou závislou oblast, která přistupuje k danému správci front IBM MQ . Chcete-li to provést, musíte vytvořit člena subsystému (SSM) v IMS.Knihovna PROCLIB a identifikujte SSM pro použitelné oblasti IMS .

Umístění záznamu člena subsystému do adresáře IMS.PROCLIB

Každá položka SSM v souboru IMS.PROCLIB definuje připojení z oblasti IMS k jinému správci front.

Chcete-li pojmenovat modul SSM, zřetězte hodnotu (jeden až čtyři alfanumerické znaky) pole IMSID makra CTRL systému IMS IMSs libovolným názvem (jeden až čtyři alfanumerické znaky) definovaným vaším serverem.

Jeden modul SSM může být sdílen všemi oblastmi IMS nebo pro každý region může být definován specifický člen. Tento člen obsahuje tolik záznamů, kolik existuje připojení k externím subsystémům. Každý záznam je 80znakový záznam.

Poziční parametry

Pole v této položce jsou:

```
SSN,LIT,ESMT,RTT,REO,CRC
```

kde:

SSN
Určuje název správce front IBM MQ . Je povinný a musí obsahovat jeden až čtyři znaky.

LIT:
Určuje token jazykového rozhraní (LIT) dodaný produktu IMS. Toto pole je povinné, jeho hodnota se musí shodovat s hodnotou v modulu CSQQDEFV.

ESMT
Určuje tabulku modulu externího subsystému (ESMT). Tato tabulka určuje, které moduly příloh musí být načteny produktem IMS. CSQQESMT je požadovaná hodnota pro toto pole.

RTT
Tato volba není podporována produktem IBM MQ.

REO-
Uvádí volbu REO (region error option), která se má použít, pokud aplikace IMS odkazuje na externí subsystém, který není v provozu, nebo pokud prostředky nejsou k dispozici v době vytvoření podprocesu. Toto pole je volitelné a obsahuje jeden znak, který může být:

R
Předá návratový kód aplikaci, což označuje, že požadavek na služby IBM MQ selhal.

Q
Ukončí aplikaci s nestandardním kódem U3051, odvolá aktivitu do posledního bodu potvrzení, provede operaci PSTOP transakce a vyžádá si vstupní zprávu. Tato volba se použije pouze v případě, že se aplikace IMS pokusí odkazovat na externí subsystém, který není v provozu, nebo pokud nejsou prostředky k dispozici v době vytvoření podprocesu.

Kódy dokončení a příčiny IBM MQ jsou vráceny aplikaci, pokud dojde k problému IBM MQ během zpracování IBM MQ požadavku; to znamená poté, co adaptér předal požadavek na IBM MQ.

A
Ukončí aplikaci s nestandardním kódem U3047 a zruší vstupní zprávu. Tato volba platí pouze v případě, že aplikace IMS odkazuje na externí subsystém, který není v provozu, nebo pokud nejsou prostředky k dispozici v době vytvoření podprocesu.

Kódy dokončení a příčiny IBM MQ jsou vráceny aplikaci, pokud dojde k problému IBM MQ během zpracování IBM MQ požadavku; to znamená poté, co adaptér předal požadavek na IBM MQ.

CRC
Tuto volbu lze zadat, ale produkt IBM MQji nepoužívá.

Poznámka: Úplné podrobnosti o všech pozičních parametrech viz Jak jsou externí subsystémy uvedeny v IMS.

Příkladem položky SSM je:

```
CSQ1,MQM1,CSQQESMT,,R,
```

kde:

CSQ1	Výchozí název subsystému dodaný s IBM MQ. Toto můžete změnit tak, aby vyhovovalo vaší instalaci.
MQM1	Výchozí hodnota LIT dodaná v CSQQDEFV.

CSQQESMT	Název modulu externího subsystému. Tuto hodnotu musíte použít.
R	Volba příkazu REO.

Parametry klíčových slov

Parametry IBM MQ lze zadat ve formátu klíčového slova. Parametr SST může mít hodnotu DB2 nebo MQ. Podpora pro hodnotu MQ byla přidána do IMS 14. Použití produktu MQ usnadňuje srozumitelnost a příkaz subsystému IMS nyní obsahuje hodnotu SST, ale jinak nemá žádný významný účinek.
V případě potřeby lze i nadále použít hodnotu DB2 . Další parametry jsou popsány v části Poziční parametrya jsou uvedeny v následujícím příkladu:

```
SST=MQ,SSN=SYS3,LIT=MQM3,ESMT=CSQQESMT
```

kde:

SYS3	Název subsystému
MQM3	LIT, jak je dodáváno v CSQQDEFV
CSQQESMT	Název modulu externího subsystému

Určení parametru SSM EXEC

Zadejte parametr SSM EXEC ve spouštěcí proceduře řídicí oblasti IMS . Tento parametr určuje jednoznakový až čtyřznakový název člena subsystému (SSM).

Zadáte-li modul SSM pro řídicí oblast IMS , může se jakákoli závislá oblast spuštěná pod řídicí oblastí připojit ke správci front produktu IBM MQ uvedenému v souboru IMS.Člen PROCLIB určený parametrem SSM. Soubor IMS.Název člena PROCLIB je IMS ID (IMSID= *xxxx*) zřetězené s jedním až čtyřmi znaky uvedenými v parametru SSM EXEC. IMS ID je parametr ID IMSmakra generování IMSCTRL.

Produkt IMS vám umožňuje definovat tolik připojení externího subsystému, kolik je požadováno. Pro různé správce front IBM MQ lze definovat více než jedno připojení. Všechna připojení IBM MQ musí být ve stejném systému z/OS . Pro závislou oblast můžete uvést závislou oblast SSM nebo použít oblast zadanou pro řídicí oblast. V SSM závislé oblasti a SSM řídicí oblasti můžete zadat různé volby chyb oblasti (REO). Tabulka 67 na stránce 984 ukazuje různé možnosti specifikací SSM.

Tabulka 67. Volby specifikace SSM

SSM pro řídicí oblast	SSM pro závislou oblast	Akce	Komentář
Ne	Ne	Není	Nelze připojit žádný externí subsystém.
Ne	Ano	Není	Nelze připojit žádný externí subsystém.
Ano	Ne	Použít řídicí oblast SSM	Aplikace naplánované v oblasti mohou přistupovat k externím subsystémům identifikovaným v řídicí oblasti SSM. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do adresních prostorů řídicí oblasti a závislé oblasti.
Ano	Ano (prázdné)	Pro závislou oblast se nepoužívá žádný modul SSM.	Aplikace naplánované v této oblasti mohou přistupovat pouze k databázím DL/I. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do adresního prostoru řídicí oblasti.

Tabulka 67. Volby specifikace SSM (pokračování)			
SSM pro řídicí oblast	**SSM pro závislou oblast**	**Akce**	**Komentář**
Ano	Ano (není prázdné)	Zkontrolujte závislou oblast SSM s řídicí oblastí SSM	Aplikace naplánované v této oblasti mohou přistupovat pouze k externím subsystémům identifikovaným v obou SSM. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do adresních prostorů řídicí oblasti a závislé oblasti.

Neexistuje žádný specifický parametr pro řízení maximálního počtu možností specifikace SSM.

Předběžné načtení adaptéru IMS

Výkon adaptéru IMS lze zlepšit, pokud je předem načten produktem IMS. Předběžné načtení je řízeno členem DFSMPLxx IMS.PROCLIB: viz " IMS Příručka pro administraci: Systém " pro další informace. Názvy modulů IBM MQ , které mají být zadány, jsou:

CSQACLST	CSQAMLST	CSQAPRH	CSQAVICM	CSQFSALM	CSQQDEFV
CSQQCONN	CSQQDISC	CSQQTERM	CSQQINIT	CSQQBACK	CSQQCMMT
CSQQESMT	CSQQPREP	CSQQTTHD	CSQQWAIT	CSQQNORM	CSQQSSOF
CSQQSSON	CSQFSTAB	CSQQRESV	CSQQSNOP	CSQQCMND	CSQQCVER
CSQQTMID	CSQQTRGI	CSQQCON2	Rozhraní CSQBPAPI	CSQBCRMH	CSQBAPPL

Další informace o použití produktu IBM MQ classes for JMSviz téma Použití IBM MQ classes for JMS v IMS.

Aktuální verze modulů IMS podporujících předběžné načítání IBM MQ z knihoven formátu PDS-E pouze v oblastech MPP, BMP, IFP, JMP a JBP. Jakýkoli jiný typ oblasti IMS nepodporuje předběžné načtení z knihoven PDS-E. Je-li pro jakýkoli jiný typ oblasti vyžadováno předběžné načtení, musí být poskytnuté moduly IBM MQ zkopírovány do knihovny formátu PDS.

z/OS *Definování správců front IBM MQ pro adaptér IMS*

Názvy správců front IBM MQ a jejich odpovídající tokeny LIT (language interface tokeny) musí být definovány v tabulce definic správců front.

Pomocí dodaného makra CSQQDEFX vytvořte zaváděcí modul CSQQDEFV. Obrázek 118 na stránce 985 ukazuje syntaxi tohoto makra assembleru.

```
CSQQDEFX TYPE=ENTRY|DEFAULT,NAME=qmgr-name,LIT=token
or
CSQQDEFX TYPE=END
```

Obrázek 118. Syntaxe makra CSQQDEFX

Parametry

TYP=POLOŽKA | PŘEDVOLBA
Zadejte buď TYPE=ENTRY, nebo TYPE=DEFAULT následujícím způsobem:

TYP=POLOŽKA
Určuje, že má být vygenerována položka tabulky popisující správce front IBM MQ , který je k dispozici pro aplikaci IMS . Pokud se jedná o první položku, vygeneruje se také záhlaví tabulky, včetně příkazu CSECT CSQQDEFV.

TYPE=VÝCHOZÍ
Jako pro TYPE=ENTRY. Zadaný správce front je výchozím správcem front, který má být použit v případě, že MQCONN nebo MQCONNX určuje název, který je prázdný. V tabulce musí být pouze jedna taková položka.

NAME= *název_správce front*
Určuje název správce front určený pomocí parametru **MQCONN** nebo **MQCONNX**.

LIT = token
Určuje název tokenu jazykového rozhraní (LIT), který produkt IMS používá k identifikaci správce front.

Volání MQCONN nebo MQCONNX přidruží vstupní parametr *name* a výstupní parametr *hconn* k návěští názvu, a tedy k LIT v položce CSQQDEFV. Další volání IBM MQ , která předávají parametr *hconn* , používají LIT z položky CSQQDEFV identifikované ve volání MQCONN nebo MQCONNX pro přímá volání do správce front IBM MQ definovaného ve členu IMS SSM PROCLIB se stejným LIT.

Souhrnně řečeno, parametr **name** ve volání MQCONN nebo MQCONNX identifikuje LIT v CSQQDEFV a stejný LIT ve členu SSM identifikuje správce front IBM MQ . (Informace o volání MQCONN naleznete v tématu MQCONN-Connect queue manager. Informace o volání MQCONNX naleznete v tématu MQCONNX-Connect queue manager (extended).)

TYPE=END
Určuje, že tabulka je dokončena. Pokud je tento parametr vynechán, předpokládá se TYPE=ENTRY.

Použití makra CSQQDEFX

V tabulce Obrázek 119 na stránce 986 je zobrazeno obecné rozvržení tabulky definic správců front.

```
CSQQDEFX NAME=subsystem1,LIT=token1
CSQQDEFX NAME=subsystem2,LIT=token2,TYPE=DEFAULT
CSQQDEFX NAME=subsystem3,LIT=token3
...
CSQQDEFX NAME=subsystemN,LIT=tokenN
CSQQDEFX TYPE=END
END
```

Obrázek 119. Rozvržení definiční tabulky správce front

z/OS *Nastavení monitoru spouštěčů IMS*

Můžete nastavit dávkově orientovaný program IMS pro monitorování inicializační fronty IBM MQ .

Definujte aplikaci pro IMS pomocí modelu CSQQTAPL v knihovně thlqual.SCSQPROC (viz Příklad definice transakce pro CSQQTRMN).

Vygenerujte PSB a ACB pomocí modelu CSQQTPSB v knihovně thlqual.SCSQPROC (viz Příklad definice PSB pro CSQQTRMN).

```
*  This is the application definition *
*  for the IMS Trigger Monitor BMP    *

APPLCTN PSB=CSQQTRMN,
PGMTYPE=BATCH,
SCHDTYP=PARALLEL
```

Obrázek 120. Příklad definice transakce pro CSQQTRMN

```
PCB  TYPE=TP,      ALTPCB for transaction messages
MODIFY=YES,        To "triggered" IMS transaction
PCBNAME=CSQQTRMN
PCB  TYPE=TP,      ALTPCB for diagnostic messages
MODIFY=YES,        To LTERM specified or "MASTER"
PCBNAME=CSQQTRMG,
EXPRESS=YES
PSBGEN LANG=ASSEM,
PSBNAME=CSQQTRMN,  Runs program CSQQTRMN
CMPAT=YES
```

Obrázek 121. Příklad definice PSB pro CSQQTRMN

Další informace o spuštění a zastavení monitoru spouštěčů IMS naleznete v tématu Řízení IMS monitoru spouštěčů.

z/OS Nastavení mostu IMS

Most IBM MQ - IMS je volitelná komponenta, která umožňuje produktu IBM MQ vstup a výstup do a z existujících programů a transakcí, které nejsou IBM MQpovoleny.

Toto téma popisuje, co musíte udělat pro přizpůsobení mostu IBM MQ - IMS .

Definujte parametry XCF a OTMA pro IBM MQ.
Tento krok definuje názvy skupin a členů XCF pro systém IBM MQ a další parametry OTMA. IBM MQ a IMS musí patřit do stejné skupiny XCF. K přizpůsobení těchto parametrů v zaváděcím modulu parametrů systému použijte klíčové slovo OTMACON makra CSQ6SYSP .

Další informace viz Použití CSQ6SYSP .

Definujte parametry XCF a OTMA pro IMS.
Tento krok definuje názvy skupin a členů XCF pro systém IMS . IMS a IBM MQ musí patřit do stejné skupiny XCF.

Přidejte následující parametry do svého seznamu parametrů IMS , buď ve svém JCL, nebo ve členu DFSPBxxx v IMS PROCLIB:

OTMA=Y
Toto spustí OTMA automaticky při spuštění IMS . (Je volitelné, pokud zadáte OTMA=N, můžete také spustit OTMA zadáním příkazu IMS /START OTMA.)

GRNAME=
Tento parametr udává název skupiny XCF.

Je stejný jako název skupiny zadaný v definici paměťové třídy (viz další krok) a v parametru **Group** klíčového slova OTMACON makra CSQ6SYSP .

OTMANM=
Tento parametr udává název člena XCF systému IMS .

Toto je stejné jako název člena uvedený v definici paměťové třídy (viz další krok).

Sdělte IBM MQ název skupiny XCF a název člena systému IMS .
Tato hodnota je určena paměťovou třídou fronty. Chcete-li odesílat zprávy přes most IBM MQ - IMS , musíte tuto volbu zadat při definování paměťové třídy pro frontu. V paměťové třídě musíte definovat skupinu XCF a název člena cílového systému IMS . Chcete-li to provést, použijte buď operace IBM MQ a ovládací panely, nebo použijte příkazy IBM MQ , jak je popsáno v tématu Úvod do programovatelných formátů příkazů.

Nastavte požadované zabezpečení.
Příkaz /SECURE OTMA IMS určuje úroveň zabezpečení, která má být použita pro **každého** IBM MQ správce front, který se připojuje k produktu IMS prostřednictvím OTMA. Další informace naleznete v tématu Aspekty zabezpečení pro použití produktu IBM MQ s produktem IMS .

Přidání dalšího připojení IMS ke stejnému správci front

Chcete-li přidat připojení IMS ke stejnému správci front, musíte definovat druhou paměťovou třídu (STGCLASS) tak, aby ukazovala na nový IMS; další informace viz DEFINE STGCLASS .

Důležité:

- Jedna lokální fronta nemůže ukazovat na dvě paměťové třídy.
- Jedna paměťová třída nemůže ukazovat na dva mosty IMS .
- IBM MQ a IMS musí patřit do stejné skupiny XCF. K přizpůsobení těchto parametrů v zaváděcím modulu parametrů systému použijte klíčové slovo OTMACON makra CSQ6SYSP .

  Další informace viz Použití CSQ6SYSP .

Související pojmy
IBM MQ a IMS
“Nastavení adaptéru IMS” na stránce 981
Použití IBM MQ v rámci produktu IMS vyžaduje adaptér IBM MQ - IMS (obecně označovaný jako adaptér IMS).

IMS a IMS přemostění aplikací na IBM MQ for z/OS

z/OS Použití IBM MQ s CICS

Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér IBM MQ CICS a volitelně komponenty produktu IBM MQ CICS bridge .

Další informace o konfiguraci adaptéru IBM MQ CICS a komponent produktu IBM MQ CICS bridge naleznete v části Konfigurace připojení k produktu MQ v dokumentaci k produktu CICS .

Související pojmy
IBM MQ a CICS
“Použití IBM MQ s IMS” na stránce 980
Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

Související odkazy
“Upgrade a použití služby v prostředí Language Environment nebo z/OS Callable Services” na stránce 988
Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a podle vaší verze SMP/E.

z/OS Upgrade a použití služby v prostředí Language Environment nebo z/OS Callable Services

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a podle vaší verze SMP/E.

Následující tabulky ukazují, co je třeba udělat s produktem IBM MQ for z/OS , pokud upgradujete svou úroveň nebo použijete službu na následující produkty:

- Jazykové prostředí
- z/OS Callable Services (například APPC a RRS)

Tabulka 68. Služba byla použita nebo produkt byl upgradován na nové vydání

Produkt	**Akce při použití CALLLIBS a SMP/E V3r2 nebo novější** **Poznámka: Nemusíte spouštět oddělené úlohy pro jazykové prostředí a volatelné služby. Jedna práce bude stačit.**	**Akce, pokud používáte LINK**
Jazykové prostředí	1. Nastavte hranici úlohy SMP/E na cílovou zónu. 2. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako např. CHECK, RETRY (YES) a RC. Další informace viz *z/OS Příkazy SMP/E* . 3. Spusťte úlohu SMP/E.	Není vyžadována žádná akce za předpokladu, že zóny SMP/E byly nastaveny pro automatické opětovné propojení a byla spuštěna úloha CSQ8SLDQ .
Volatelné služby	1. Nastavte hranici úlohy SMP/E na cílovou zónu. 2. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako např. CHECK, RETRY (YES) a RC. Další informace viz *z/OS Příkazy SMP/E* . 3. Spusťte úlohu SMP/E.	Není vyžadována žádná akce za předpokladu, že zóny SMP/E byly nastaveny pro automatické opětovné propojení a byla spuštěna úloha CSQ8SLDQ .

Tabulka 69. Jeden z produktů byl aktualizován na nové vydání v novém prostředí a knihovnách SMP/E		
Produkt	**Akce při použití CALLLIBS a SMP/E V3r2 nebo novější** **Poznámka: Pro jazykové prostředí a volatelné služby nemusíte spouštět tři samostatné úlohy. Jedna práce bude stačit pro oba produkty.**	**Akce, pokud používáte LINK**
Jazykové prostředí	1. Změňte DDDEFs pro SCEELKED a SCEESPC tak, aby ukazovaly na novou knihovnu. 2. Nastavte hranici úlohy SMP/E na cílovou zónu. 3. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako např. CHECK, RETRY (YES) a RC. Další informace viz *z/OS Příkazy SMP/E* . 4. Spusťte úlohu SMP/E.	1. Odstraňte podpoložky XZMOD pro následující položky LMOD v cílové zóně IBM MQ for z/OS : CMQXDCST, CMQXRCTL, CMQXSUPR, CSQCBE00, CSQCBE30, CSQCBP00, CSQCBP10, CSQCBR00, CSQUCVX, CSQUDLQH, CSQVXSPT, CSQXDCST, CSQXRCTL, CSQXSUPR, CSQXTCMI, CSQXTCP, CSQXQTNSV, C$tag13 CSQ7DR 2. Nastavte odpovídající značky ZONEINDEXs mezi zónami IBM MQ a zónami jazykového prostředí. 3. Upravte CSQ8SLDQ tak, aby odkazoval na novou zónu v parametru FROMZONE příkazů LINK. CSQ8SLDQ lze nalézt v knihovně SCSQINST. 4. Spusťte příkaz CSQ8SLDQ.
Volatelné služby	1. Změňte DDDEF pro CSSLIB tak, aby ukazoval na novou knihovnu 2. Nastavte hranici úlohy SMP/E na cílovou zónu. 3. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako např. CHECK, RETRY (YES) a RC. Další informace viz *z/OS Příkazy SMP/E* . 4. Spusťte úlohu SMP/E.	1. Odstraňte podpoložky XZMOD pro následující položky LMOD v cílové zóně IBM MQ for z/OS : CMQXRCTL, CMQXSUPR, CSQBSRV, CSQILPLM, CSQXJST, CSQXRCTL, CSQXSUPR, CSQ3AMGP, CSQ3EPX, CSQ3REPL 2. Nastavte odpovídající hodnoty ZONEINDEXs mezi zónami IBM MQ a zónami Callable Services. 3. Upravte CSQ8SLDQ tak, aby odkazoval na novou zónu v parametru FROMZONE příkazů LINK. CSQ8SLDQ lze nalézt v knihovně SCSQINST. 4. Spusťte příkaz CSQ8SLDQ.

Příklad úlohy pro opětovné propojení modulů při použití CALLLIBS viz “Spuštění úlohy LINK CALLLIBS” na stránce 990.

z/OS Spuštění úlohy LINK CALLLIBS

Vzorová úloha pro opětovné propojení modulů při použití CALLLIBS.

Následuje příklad úlohy opětovného propojení modulů při použití knihoven CALLLIB v systému SMP/E V3r2 . Musíte zadat JOBCARD a název datové sady SMP/E CSI, který obsahuje IBM MQ for z/OS.

```
//*******************************************************************
//* RUN LINK CALLLIBS.
//*******************************************************************
//CALLLIBS EXEC PGM=GIMSMP,REGION=4096K
//SMPCSI  DD DSN=your.csi
//       DISP=SHR
//SYSPRINT DD SYSOUT=*
//SMPCNTL DD *
SET BDY(TZONE).
LINK LMODS CALLLIBS .
/*
```

Obrázek 122. Příklad úlohy SMP/E LINK CALLLIBS

z/OS Použití uživatelských procedur OTMA v adresáři IMS

Toto téma použijte, chcete-li použít uživatelské procedury IMS Open Transaction Manager Access s produktem IBM MQ for z/OS.

Chcete-li odeslat výstup z transakce IMS do IBM MQa tato transakce nepochází z IBM MQ, musíte kódovat jednu nebo více uživatelských procedur OTMA IMS .

Podobně, chcete-li odeslat výstup do cíle, který není OTMA, a transakce pochází z IBM MQ, musíte také kódovat jednu nebo více uživatelských procedur OTMA IMS .

V produktu IMS jsou k dispozici následující uživatelské procedury, které vám umožní upravit zpracování mezi IMS a IBM MQ:

- Uživatelská procedura před směrováním OTMA
- Uživatelská procedura DRU (destination resolution user)

Názvy uživatelských procedur OTMA

Musíte pojmenovat uživatelskou proceduru před směrováním DFSYPRX0. Uživatelskou proceduru DRU můžete pojmenovat libovolně, pokud to není v konfliktu s názvem modulu, který je již v adresáři IMS.

Určení názvu uživatelské procedury rozpoznání místa určení

Pomocí parametru *Druexit* klíčového slova OTMACON makra CSQ6SYSP můžete určit název uživatelské procedury OTMA DRU, kterou má spustit IMS.

Chcete-li zjednodušit identifikaci objektů, zvažte přijetí konvence pojmenování DRU0xxxx, kde xxxx je název vašeho správce front IBM MQ .

Pokud neuvedete název uživatelské procedury DRU v parametru OTMACON, předvolba je DFSYDRU0. Další informace viz DFSYDRU0 .

Konvence pojmenování pro cíl IMS

Potřebujete konvenci pojmenování pro místo určení, kam odesíláte výstup ze svého programu IMS . Toto je místo určení, které je nastaveno ve volání CHNG vaší aplikace IMS , nebo které je přednastaveno v IMS PSB.

Ukázkový scénář pro ukončení OTMA

Příklad uživatelské procedury před směrováním a cílové uživatelské procedury směrování pro systém IMSnaleznete v následujících tématech:

- “Uživatelská procedura před směrováním DFSYPRX0” na stránce 992

- “Uživatelská procedura rozpoznání cíle” na stránce 993

Chcete-li zjednodušit identifikaci, nastavte název místa určení OTMA podobně jako název správce front IBM MQ , například název správce front IBM MQ se opakuje. V tomto případě, pokud je název správce front IBM MQ " **VCPE** ", cíl nastavený voláním CHNG je" **VCPEVCPE** ".

Související pojmy

IBM MQ a IMS

“Použití IBM MQ s IMS” na stránce 980

Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

IMS a IMS přemostění aplikací na IBM MQ for z/OS

z/OS Uživatelská procedura před směrováním DFSYPRX0

Toto téma obsahuje ukázkovou uživatelskou proceduru před směrováním pro OTMA v adresáři IMS.

Nejprve musíte kódovat uživatelskou proceduru před směrováním DFSYPRX0. Parametry předané této rutině uživatelem IMSviz Uživatelská procedura OTMA Destination Resolution (DFSYPRX0 a další uživatelské procedury typu OTMAYPRX) .

Tato procedura testuje, zda je zpráva určena pro známé místo určení OTMA (v našem příkladu VCPEVCPE). Pokud ano, musí uživatelská procedura zkontrolovat, zda transakce odesílající zprávu pochází z OTMA. Pokud zpráva pochází z OTMA, bude mít záhlaví OTMA, takže byste měli ukončit DFSYPRX0 s registrem 15 nastaveným na nulu.

- Pokud transakce odesílající zprávu nepochází z OTMA, musíte nastavit jméno klienta jako platného klienta OTMA. Jedná se o název člena XCF správce front IBM MQ , kterému chcete odeslat zprávu. Měli byste nastavit název klienta (v parametru OTMACON makra CSQ6SYSP) na název správce front. Toto nastavení je výchozí. Pak byste měli ukončit DFSYPRX0 nastavení registru 15 až 4.
- Pokud transakce odesílající zprávu pochází z OTMA a cíl není OTMA, měli byste nastavit registraci 15 na 8 a ukončit.
- Ve všech ostatních případech byste měli nastavit registr 15 na nulu.

Nastavíte-li název klienta OTMA na ten, který není znám produktu IMS, volání CHNG nebo ISRT vaší aplikace vrátí stavový kód A1 .

V případě systému IMS , který komunikuje s více než jedním správcem front IBM MQ , byste měli opakovat logiku pro každého správce front IBM MQ .

Ukázkový kód asembleru je uveden v souboru Obrázek 123 na stránce 993:

```
TITLE 'DFSYPRX0: OTMA PRE-ROUTING USER EXIT'
DFSYPRX0 CSECT
DFSYPRX0 AMODE 31
DFSYPRX0 RMODE ANY
*
SAVE (14,12),,DFSYPRX0&SYSDATE&SYSTIME
SPACE 2
LR  R12,R15        MODULE ADDRESSABILITY
USING DFSYPRX0,R12
*
L   R2,12(,R1)      R2 -> OTMA PREROUTE PARMS
*
LA  R3,48(,R2)      R3 AT ORIGINAL OTMA CLIENT (IF ANY)
CLC  0(16,R3),=XL16'00'  OTMA ORIG?
BNE  OTMAIN        YES, GO TO THAT CODE
*
NOOTMAIN DS 0H            NOT OTMA INPUT
LA  R5,8(,R2)       R5 IS AT THE DESTINATION NAME
CLC  0(8,R5),=C'VCPEVCPE' IS IT THE OTMA UNSOLICITED DEST?
BNE  EXIT0         NO, NORMAL PROCESSING
*
L   R4,80(,R2)      R4 AT ADDR OF OTMA CLIENT
MVC  0(16,R4),=CL16'VCPE' CLIENT OVERRIDE
B   EXIT4         AND EXIT
*
OTMAIN  DS 0H           OTMA INPUT
LA  R5,8(,R2)       R5 IS AT THE DESTINATION NAME
CLC  0(8,R5),=C'VCPEVCPE' IS IT THE OTMA UNSOLICITED DEST?
BNE  EXIT8         NO, NORMAL PROCESSING
```

```
*
EXIT0  DS 0H
LA  R15,0         RC = 0
B   BYEBYE
*
EXIT4  DS 0H
LA  R15,4         RC = 4
B   BYEBYE
*
EXIT8  DS 0H
LA  R15,8         RC = 8
B   BYEBYE
*
BYEBYE  DS 0H
RETURN (14,12),,RC=(15)   RETURN WITH RETURN CODE IN R15
SPACE 2
REQUATE
SPACE 2
END
```

Obrázek 123. Ukázka sestavovacího modulu uživatelské procedury před směrováním OTMA

z/OS Uživatelská procedura rozpoznání cíle

Toto téma obsahuje ukázku uživatelské procedury rozpoznání místa určení pro IMS.

Pokud jste nastavili registry 15 až 4 v DFSYPRX0, nebo pokud byl zdrojem transakce OTMA ***a*** jste nastavili Registrovat 15 na nulu, bude vyvolána uživatelská procedura DRU. V tomto příkladu je název uživatelské procedury DRU DRU0VCPE.

Uživatelská procedura DRU zkontroluje, zda je cíl VCPEVCPE. Pokud ano, nastaví uživatelská data OTMA (v předponě OTMA) takto:

Offset
Uživatelská data OTMA

(desetinné)

0
Délka uživatelských dat OTMA (v tomto příkladu 334)

2
MQMD

326
Odpovědět na formát

Tyto odchylky jsou místem, kde most IBM MQ - IMS očekává tyto informace.

Uživatelská procedura DRU by měla být co nejjednodušší. Proto jsou v této ukázce všechny zprávy pocházející z produktu IMS pro konkrétního správce front IBM MQ vloženy do stejné fronty IBM MQ .

Pokud musí být zpráva trvalá, IMS musí používat synchronizované propojení procesů transakcí. Chcete-li to provést, musí uživatelská procedura DRU nastavit příznak OUTPUT. Další informace viz Určení synchronizovaných propojení procesů pro IBM MQ .

Napište aplikaci IBM MQ ke zpracování této fronty a použijte informace ze struktury MQMD, struktury MQIIH (je-li k dispozici) nebo uživatelských dat ke směrování každé zprávy do jejího cíle.

Ukázková uživatelská procedura jednotky DRU asembleru je zobrazena v souboru Obrázek 124 na stránce 994.

```
TITLE 'DRU0VCPE: OTMA DESTINATION RESOLUTION USER EXIT'
DRU0VCPE CSECT
DRU0VCPE AMODE 31
DRU0VCPE RMODE ANY
*
SAVE (14,12),,DRU0VCPE&SYSDATE&SYSTIME
SPACE 2
LR  R12,R15            MODULE ADDRESSABILITY
USING DRU0VCPE,R12
*
L   R2,12(,R1)           R2 -> OTMA DRU PARMS
*
L   R5,88(,R2)           R5 ADDR OF OTMA USERDATA
LA  R6,2(,R5)           R6 ADDR OF MQMD
USING MQMD,R6            AS A BASE
*
LA  R4,MQMD_LENGTH+10       SET THE OTMA USERDATA LEN
STH  R4,0(,R5)           = LL + MQMD + 8
*                       CLEAR REST OF USERDATA
MVI  0(R6),X'00'          ...NULL FIRST BYTE
MVC  1(255,R6),0(R6)        ...AND PROPAGATE IT
MVC  256(MQMD_LENGTH-256+8,R6),255(R6) ...AND PROPAGATE IT
*
VCPE   DS  0H
CLC  44(16,R2),=CL16'VCPE'     IS DESTINATION VCPE?
BNE  EXIT4             NO, THEN DEST IS NON-OTMA
MVC  MQMD_REPLYTOQ,=CL48'IMS.BRIDGE.UNSOLICITED.QUEUE'
MVC  MQMD_REPLYTOQMGR,=CL48'VCPE'  SET QNAME AND QMGRNAME
MVC  MQMD_FORMAT,MQFMT_IMS     SET MQMD FORMAT NAME
MVC  MQMD_LENGTH(8,R6),MQFMT_IMS_VAR_STRING
*                       SET REPLYTO FORMAT NAME
B   EXIT0
*
EXIT0  DS  0H
LA  R15,0             SET RC TO OTMA PROCESS
B   BYEBYE             AND EXIT
*
EXIT4  DS  0H
LA  R15,4             SET RC TO NON-OTMA
B   BYEBYE             AND EXIT
*
BYEBYE  DS  0H
RETURN (14,12),,RC=(15)       RETURN CODE IN R15
SPACE 2
REQUATE
SPACE 2
CMQA  EQUONLY=NO
CMQMDA DSECT=YES
SPACE 2
END
```

Obrázek 124. Uživatelská procedura DRU ukázkového asembleru

z/OS Použití produktu IBM z/OSMF k automatizaci IBM MQ

IBM z/OS Management Facility (z/OSMF) poskytuje funkce správy systému v uživatelském rozhraní orientovaném na úlohy, které je založeno na webovém prohlížeči, s integrovanou podporou uživatelů, takže můžete snáze spravovat každodenní provoz a administraci systémů z/OS na sálových počítačích.

Optimalizací některých tradičních úloh a automatizací jiných úloh může produkt z/OSMF pomoci zjednodušit některé oblasti správy systému z/OS .

Prostředky lze zajistit nebo dezajistit klepnutím na tlačítko z portálu poskytnutého uživatelem. Produkt z/OSMF poskytuje rozhraní REST API, která vám pomohou s touto úlohou.

Ukázkový portál tržiště dodávaný s produktem z/OSMF lze také použít k zajištění a zrušení zajišťování prostředků. Zkušenější uživatelé mohou také používat webové uživatelské rozhraní (WUI) z/OSMF .

Tento oddíl předpokládá, že rozumíte produktu z/OSMF, ale pokud nejste obeznámeni s produktem z/OSMF , měli byste si přečíst téma Začínáme s produktem z/OSMF. Alternativně můžete k této sekci přistoupit z online nápovědy produktu z/OSMF WUI.

Měli byste se seznámit s konfigurací produktu z/OS Cloud, tj.:

- Zajišťování cloudu- Služby správy prostředků
- Správa pracovní zátěže-další informace naleznete v příručce IBM z/OS Management Facility Programming Guide .
- Začínáme-viz *Výukový program Začínáme-Cloud*

z/OSMF 2.2 zavádí aktivity a úlohy založené na rolích, takže je důležité, abyste porozuměli konceptům, jako jsou:

domény
administrátoři
schvalovatelé
tenanti
šablony
instance
sledy prací

a tak dále.

K dispozici jsou ukázkové sledy prací a přidružené soubory produktu IBM MQ z/OSMF , které lze nainstalovat jako součást funkce IBM MQ for z/OS UNIX System Services Components . Proces instalace této funkce a struktura adresářů a souborů jsou popsány v části IBM MQ for z/OS Adresář programu. Odkazy ke stažení pro adresáře programů viz IBM MQ for z/OS Soubory PDF adresáře programů.

Ukázkové sledy prací jsou napsány v jazyce XML a demonstrují, jak automatizovat zajišťování (vytvoření) nebo zrušení zajišťování (zničení) správců front IBM MQ , inicializátorů kanálů a lokálních front a jak provádět akce se zajišťovanými prostředky IBM MQ . Kroky v rámci sledů prací odesílají úlohy (JCL), spouštějí spustitelné soubory REXX, skripty shellu procesu nebo vydávají volání REST API .

Ukázky jsou navrženy tak, aby ilustrovaly typy funkcí, kterých lze dosáhnout pomocí produktu z/OSMF. Předpokládá se, že sledy prací z/OSMF budou obecně použity k zajištění prostředků a akce, jako je vložení nebo získání zprávy, budou v podstatě prováděny pomocí aplikací IBM MQ .

Můžete spustit ukázkové sledy prací tak, jak byly dodány, za předpokladu, že byly nastaveny vlastnosti proměnné sledu prací (jak je popsáno v následujících sekcích), nebo je můžete upravit podle potřeby. Chcete-li provádět další funkce, můžete raději napsat vlastní sledy prací. Před spuštěním ukázkových sledů prací viz:

- “Předpoklady pro z/OSMF” na stránce 996
- “Nastavení zabezpečení” na stránce 997
- “Omezení” na stránce 999

Ukázkové aplikace sledu prací jsou poskytovány pro:

- “Automatizujte zajišťování nebo zrušení zajišťování správců front IBM MQ a provádějte akce pro zajišťované správce front.” na stránce 1001
- “Automatizujte zajišťování nebo zrušení zajišťování lokálních front IBM MQ a proveďte akce pro zajištěné fronty.” na stránce 1002.

Související pojmy

“nastaveníIBM MQ for z/OS” na stránce 876
Toto téma použijte jako průvodce krok za krokem pro přizpůsobení systému IBM MQ for z/OS .

z/OS Předpoklady pro z/OSMF

Nezbytné předpoklady, které potřebujete ke spuštění IBM z/OS Management Facility (z/OSMF) s IBM MQ

Sledy prací dodávané v produktu IBM MQ for z/OS 9.1.0 využívají novou funkci v produktu z/OSMF, který je poskytován prostřednictvím oprav APAR na obou systémech z/OS 2.1 a 2.2. Další podrobnosti jsou uvedeny v následujícím textu.

1. Správně jste nainstalovali a nakonfigurovali produkt IBM z/OS Management Facility 2.2 . Pokud spouštíte s povoleným zabezpečením, ujistěte se, že všechna nastavení zabezpečení dokumentovaná produktem z/OSMF byla nakonfigurována.
2. Nainstalovali jste následující opravy APAR pro:

   z/OS 2.1

   - PI71068
   - PI71079
   - PI71082
   - PI71084
   - OA50130

   z/OS 2.2

   - PI70526
   - PI70521
   - PI70527
   - PI67839
   - PI70767
   - PI46315
   - OA49081
   - OA49802
   - OA50130
3. Proces typu angel z/OSMF (je-li vyžadován) a procesy serveru byly nakonfigurovány.
4. Prostředí z/OS Cloud bylo nakonfigurováno (jak bylo stručně popsáno výše a zdokumentováno z/OSMF).
5. Produkt IBM MQ for z/OS 9.0.1 byl nainstalován a zaváděcí knihovny produktu jsou k dispozici.
6. Byly provedeny následující úlohy přizpůsobení správce front IBM MQ :

Úloha	Popis
1	Identifikace parametrů systému z/OS
2	Autorizace APF pro zaváděcí knihovny IBM MQ
3	Aktualizovat seznam odkazů z/OS a LPA
4	Aktualizovat tabulku vlastností programu z/OS

7. Ukázkové sledy prací a přidružené soubory jsou nainstalovány ve vhodném adresáři z/OS UNIX System Services (z/OS UNIX).
8. Adresář `/tmp` z/OS UNIX je k dispozici, protože sled prací provision.xml může v tomto adresáři vytvořit dočasný soubor. Pokud je soubor vytvořen, sled prací jej obecně po použití odstraní.
9. Soubor `deprovision.xml` obsahuje kroky, které vyvolají spustitelné soubory CSQ4ZWS1.rexx a CSQ4ZWS2.rexx REXX. Tyto spustitelné programy čekají na zastavení subsystémů správce front a inicializátoru kanálu; spustitelné programy vyvolají příkaz z/OS UNIX **SLEEP** jako systémové volání.

   V závislosti na konfiguraci produktu z/OS UNIX můžete zjistit, že příkaz **SLEEP** nefunguje jako kódovaný. Pokud během zpracování zjistíte chybu, která označuje, že příkaz **SLEEP** nebyl nalezen, můžete zkusit nahradit následující řádky v exekucích CSQ4ZWS1.rexx a CSQ4ZWS2.rexx:

```
CALL SYSCALLS('ON')             /* Enable z/OS UNIX calls    */
ADDRESS SYSCALL
"SLEEP" 10                           /* Sleep for 10 seconds */
CALL SYSCALLS 'OFF'             /* Disable z/OS UNIX calls    */
```

```
          s

'sleep' 10
```

   Poté zadejte příkaz Open MVS (OMVS) **env** a zkontrolujte nastavení proměnné prostředí PATH. Ujistěte se, že adresář, který obsahuje příkaz **sleep** , je definován v cestě PATH. Všimněte si, že příkaz **sleep** se obvykle nachází v adresáři `/bin` .
10. Ujistěte se, že byl spuštěn produkt z/OSMF .

    Procesy typu angel a server z/OSMF musí být spuštěny a musí být spuštěno uživatelské rozhraní WUI (z/OSMF Web User Interface). Další podrobnosti viz Profil Liberty: Typy procesů v systému z/OS.

    I v případě, že hodláte řídit sledy prací pomocí konzoly REST API, je třeba spustit rozhraní z/OSMF WUI. Produkt z/OSMF WUI může být užitečný pro monitorování vytváření a provádění sledů prací.

Související pojmy

“Použití produktu IBM z/OSMF k automatizaci IBM MQ” na stránce 995
IBM z/OS Management Facility (z/OSMF) poskytuje funkce správy systému v uživatelském rozhraní orientovaném na úlohy, které je založeno na webovém prohlížeči, s integrovanou podporou uživatelů, takže můžete snáze spravovat každodenní provoz a administraci systémů z/OS na sálových počítačích.

z/OS Nastavení zabezpečení

Nastavení zabezpečení požadovaná ke spuštění produktu z/OSMF.

V souboru vlastností jsou definovány následující vlastnosti proměnné ID uživatele. Další informace naleznete v tématu “Spuštění sledů prací” na stránce 1004.

Vlastnost ID uživatele	Popis
CSQ_USERID	ID uživatele použité ke spuštění kroků sledu prací. Všimněte si však, že vybrané kroky (které obecně vyžadují zvýšenou úroveň oprávnění) budou spuštěny s různými ID uživatelů na základě nastavení ID uživatelů **CSQ_ADMIN_*** uvedených v následujícím textu. Používané ID uživatele je identifikováno vlastností **runAsUser** v příslušném kroku ve sledech prací.
CSQ_ADMIN_APF_USERID	ID uživatele, které se má použít při autorizaci APF zaváděcí knihovny, která obsahuje modul parametrů systému správce front.
CSQ_APF_APPROVAL_ID	ID schválení, které umožňuje uživatelům spustit krok autorizace APF datové sady jako uživatel CSQ_ADMIN_APF_USERID.
CSQ_ADMIN_CONSOLE_USERID	ID uživatele použité při spouštění kroků pod spuštěním, které vydávají příkazy konzoly z/OS .

Vlastnost ID uživatele	Popis
	Upozornění: Tomuto ID uživatele musí být povolen přístup UPDATE k profilu spuštěné úlohy (MVS.START.STC. *) ve třídě OPERCMDS. Další informace naleznete v tématu Řízení použití příkazů operátora v dokumentaci k produktu z/OS .
CSQ_CONSOLE_APPROVAL_ID	ID schválení, které umožňuje uživatelům spouštět kroky, které spouštějí příkazy konzoly z/OS pod uživatelem CSQ_ADMIN_CONSOLE_USERID.
CSQ_ADMIN_SAF_USERID	ID uživatele, které má být použito při zadávání příkazů SAF.
CSQ_SAF_APPROVAL_ID	ID schválení, které umožňuje uživatelům spouštět kroky příkazu SAF pod uživatelem CSQ_ADMIN_SAF_USERID.
CSQ_ADMIN_SSI_USERID	ID uživatele, které se má použít při zadávání příkazu SETSSI k identifikaci subsystému zajišťovaného v produktu z/OS.
CSQ_SSI_APPROVAL_ID	ID schválení, které umožňuje uživatelům spustit krok příkazu SETSSI pod spuštěním jako uživatel CSQ_ADMIN_SSI_USERID.

Poznámka: ID uživatele používané ke spuštění sledů prací zajišťování a zrušení zajišťování musí mít dostatečná oprávnění, jak je uvedeno níže:

1. Sledy prací zajišťování a zrušení zajišťování správce front používají příkaz SETPROG k autorizaci datových sad APF. Buď je ID uživatele nastaveno ve vlastnosti CSQ_ADMIN_APF_USERID, nebo ID uživatele použité ke spuštění sledů prací musí být povoleno k zadání tohoto příkazu. Toho lze dosáhnout zadáním následujícího příkazu:

```
PERMIT MVS.SETPROG CLASS(OPERCMDS) ID(value of CSQ_ADMIN_APF_USERID) ACCESS(UPDATE)
```

   Poznámka: Příkaz SETPROG nemusí přetrvávat v rámci IPL systému z/OS , takže může být nutné ručně zadat následující příkaz SETPROG po IPL:

```
SETPROG APF,ADD,DSN=value of CSQ_AUTH_LIB_HLQ.value of CSQ_SSID.APF.LOAD,SMS
```

   Další podrobnosti o příkazu SETPROG naleznete v tématu Použití RACF k řízení seznamů APF.

   Kromě toho jste mohli povolit třídu FACILITY, aby řídila, které knihovny mohou být autorizovány APF, takže možná budete muset zadat příkaz:

```
PERMIT CSVAPF.libname CLASS(FACILITY) ID(value of CSQ_ADMIN_APF_USERID)
       ACCESS(UPDATE)
```

2. Krok ve sledu prací zajišťování správce front zadá příkaz SETSSI, který identifikuje subsystém IBM MQ pro z/OS. ID uživatele nastavené ve vlastnosti CSQ_ADMIN_SSI_USERID musí být povoleno používat tento příkaz. Toho lze dosáhnout zadáním následujícího příkazu:

```
PERMIT MVS.SETSSI.ADD CLASS(OPERCMDS) ID(value of CSQ_ADMIN_SSI_USERID)
        ACCESS(CONTROL)
```

   Poznámka: Subsystémy, které byly identifikovány pro z/OS pomocí příkazu SETSSI, netrvají v IPL systému z/OS . Proto může být nutné ručně zadat následující příkaz SETSSI po IPL:

```
SETSSI  ADD,S='value of CSQ_SSID',I=CSQ3INI,
       P='CSQ3EPX,value of CSQ_CMD_PFX,S'
```

   Další podrobnosti o příkazu SETSSI viz: Příkaz SETSSI.

3. Sledy prací zadávají příkazy správce front, takže pokud plánujete povolit zabezpečení, musí být ID uživatele nastavené ve vlastnosti CSQ_ADMIN_RACF_USERID (nebo ID uživatele používané ke spuštění sledů prací) uděleno oprávnění CLAUTH (ověření klienta) pro třídu MQADMIN nebo MXADMIN (v závislosti na používané třídě). To umožňuje tomuto ID uživatele definovat profily zabezpečení pro tyto třídy. Toho lze dosáhnout zadáním následujícího příkazu:

```
ALTUSR value of CSQ_ADMIN_RACF_USERID CLAUTH(MQADMIN)
```

   Další podrobnosti o **CLAUTH** viz Atribut CLAUTH (oprávnění třídy).
4. Sled prací deprovision.xml zadává příkazy z/OS , například úlohy DISPLAY ACTIVE, CANCEL nebo FORCE, takže ID uživatele nastavené ve vlastnosti CSQ_ADMIN_CONSOLE_USERID (nebo ID uživatele používané ke spuštění sledů prací) musí mít odpovídající oprávnění k zadávání těchto příkazů.
5. Uživatelé požadující instanci správce front, kteří používají tabulku šablon úlohy softwarových služeb, musí mít oprávnění pro přístup k funkcím z/OSMF a Asistentovi pro konfiguraci, jak definuje z/OSMF.
6. ID uživatele spotřebitele, který zajišťuje správce front, vyžaduje oprávnění k přidávání a odstraňování členů z datové sady PROCLIB definované s proměnnou CSQ_PROC_LIB.
7. Správce front musí být zajištěn před frontami zajišťování.
8. Chcete-li používat sledy prací `queueLoad.xml` a `queueOffload.xml` , musí být použité datové sady definovány předem. ID uživatele použité ke spuštění těchto sledů prací musí být také uděleno oprávnění UPDATE k datovým sadám.
9. Krok ve sledu prací `provision.xml` správce front aktuálně zakazuje zabezpečení subsystému. Úlohu `csq4znse.jcl` můžete upravit tak, aby povolovala zabezpečení subsystému, a to přidáním příslušných příkazů zabezpečení pro ochranu prostředků IBM MQ . Všimněte si však, že pokud přidáte další příkazy, musíte také přidat příkazy pro odstranění oprávnění zabezpečení v produktu `csq4dse.jcl`, který je odeslán sledem prací deprovision.xml .

   Poznámka: Tento krok vydává příkazy zabezpečení RACF . Pokud používáte alternativní produkt zabezpečení, musíte tento krok upravit a zadat odpovídající příkazy pro váš produkt zabezpečení.

Síťové požadavky

Při přidávání šablony správce front a prostředků pro šablonu je třeba klepnout na volbu **Vytvořit fond síťových prostředků**. Tím se vytvoří fond prostředků se síťovými prostředky pro tuto šablonu.

Pomocí Asistenta pro konfiguraci musí administrátor sítě dokončit tuto definici oblasti prostředků sítě definováním limitu pro počet portů, které mají být přiděleny pro tuto šablonu.

Pro každou instanci šablony sled prací `provision.xml` přidělí port v rozsahu a spustí modul listener pro naslouchání na tomto portu.

Klasifikace pomocí produktu IBM Workload Manager

Chcete-li pomocí modulu WLM klasifikovat adresní prostory správce front a inicializátoru kanálu, je třeba tuto volbu zadat při přidávání šablony pro zajišťování správce front.

Zda klasifikovat, či nikoli, je řízeno příznaky **CSQ_DEFINE_MSTR_WLM_RULE** a **CSQ_DEFINE_CHIN_WLM_RULE**, které jsou nastaveny v souboru `workflow_variables.properties`.

Další informace o klasifikaci pomocí WLM naleznete v příručce *z/OSMF Configuration Guide*.

Související pojmy

“Předpoklady pro z/OSMF” na stránce 996
Nezbytné předpoklady, které potřebujete ke spuštění IBM z/OS Management Facility (z/OSMF) s IBM MQ

z/OS Omezení

Omezení při použití z/OSMF s IBM MQ.

1. Sled prací `provision.xml` aktuálně automatizuje následující zvýrazněné úlohy přizpůsobení správce front:

Úloha	Popis
1	Identifikace parametrů systému z/OS
2	Autorizace APF pro IBM MQ zaváděcí knihovny **(provision.xml autorizuje některé knihovny APF)**
3	Aktualizovat seznam odkazů z/OS a LPA
4	Aktualizovat tabulku vlastností programu z/OS
5	**Definovat subsystém IBM MQ na z/OS**
6	**Vytvořit procedury pro IBM MQ správce front**
7	**Vytvořit procedury pro inicializátor kanálu**
8	**Definovat subsystém IBM MQ do z/OS třídy služeb WLM**
9	Vyberte a nastavte úložné prostředí odlehčování prostředku Coupling Facility.
10	Nastavení prostředku Coupling Facility
11	Implementace ovládacích prvků zabezpečení ESM
12	Aktualizujte SYS1.PARMLIB
13	**Upravit vstupní datové sady inicializace**
14	**Vytvořit datové sady zaváděcího programu a protokolu**
15	**Definovat sady stránek**
16	Přidejte položky IBM MQ do skupiny sdílení dat Db2 .
17	**Přizpůsobte moduly systémových parametrů (některé)**
18	**Přizpůsobte parametry inicializátoru kanálu (některé)**
19	Nastavení adaptérů Batch, TSO a RRS
20	Nastavení operací a ovládacích panelů
21	Zahrnout člena formátování výpisu paměti IBM MQ
22	Potlačit informační zprávy
23	Aktualizujte svého člena DIAG systému pro Advanced Message Security
24	Vytvořit procedury pro Advanced Message Security
25	Nastavení uživatele spuštěné úlohy Advanced Message Security
26	Udělte oprávnění RACDCERT administrátorovi zabezpečení pro Advanced Message Security
27	Udělit uživatelům oprávnění k prostředkům pro Advanced Message Security

2. Úlohy přizpůsobení, které nejsou zvýrazněny tučným písmem, je třeba v případě potřeby provést ručně.
3. Ukázkové členy INP1 a INP2 se momentálně používají tak, jak jsou. V případě potřeby lze definovat další vlastnosti pro řízení prostředků definovaných těmito členy.
4. Komentáře týkající se specifických vlastností uvedených v souboru vlastností označují případná omezení použití těchto vlastností. Další informace naleznete v tématu "Spuštění sledů prací" na stránce 1004.

Související pojmy

"Nastavení zabezpečení" na stránce 997
Nastavení zabezpečení požadovaná ke spuštění produktu z/OSMF.

z/OS Automatizace zajišťování objektů IBM MQ

Ukázky jsou dodávány pro automatizaci zajišťování správců front a lokálních front.

Automatizujte zajišťování nebo zrušení zajišťování správců front IBM MQ a provádějte akce pro zajišťované správce front.

K dispozici jsou následující ukázkové sledy prací z/OSMF specifické pro správce front:

Název sledu prací	Popis
provision.xml	Zajištění správce front IBM MQ for z/OS Tento ukázkový sled prací: • Zajistěte požadované systémové prostředky pro správce front. • Zabezpečí požadované systémové prostředky pro inicializátor kanálu. • Spustí správce front (který také spustí inicializátor kanálu a modul listener protokolu TCP/IP). • Spustí ukázkový ověřovací program pro instalaci správce front. Vlastnost prostředí lze nastavit tak, aby řídila zajišťování správců front s různými charakteristikami. Další informace viz téma "Spuštění sledů prací" na stránce 1004. **Poznámka:** K dispozici je soubor typu manifest (`provision.mf`), který pomáhá s přidáním šablony pro tento sled prací. Tento soubor obsahuje odkaz na soubor **qaas_readme.pdf** , který obsahuje další informace. K souboru můžete přistupovat prostřednictvím odkazu po přidání šablony.
deprovision.xml	Zrušení zajišťování správce front IBM MQ for z/OS Tento ukázkový sled prací: • Zastaví inicializátor kanálu (který také zastaví modul listener protokolu TCP/IP) a správce front. • Čeká na zastavení subsystémů • Zrušit všechna nastavení inicializátoru kanálu a systémových prostředků správce front.
startQMgr.xml	Spuštění správce front IBM MQ for z/OS Tento ukázkový sled prací spustí správce front (který také spustí inicializátor kanálu a modul listener protokolu TCP/IP).
stopQMgr.xml	Zastavit správce front IBM MQ for z/OS Tento ukázkový sled prací zastaví inicializátor kanálu (který také zastaví modul listener protokolu TCP/IP) a správce front.

Každý sled prací provede jeden nebo více kroků. Komentáře ve sledech prací vysvětlují funkci prováděnou jednotlivými kroky. Některé z těchto kroků pouze vyžadují datový vstup, zatímco některé kroky odesílají JCL, vyvolávají spustitelné soubory REXX, skripty shellu nebo vydávají volání REST API za účelem provedení uvedené funkce.

Přesný název souborů exec JCL nebo REXX naleznete v jednotlivých krocích. Sledy prací a přidružené soubory JCL nebo REXX exec odkazují na proměnné, které jsou deklarovány v jednom nebo více

proměnných souborech XML. Další informace naleznete v tématu “Soubory deklarace proměnných sledu prací” na stránce 1004.

deprovision, **startQMgr**a **stopQMgr** lze provést jako akce pro zajištěného správce front IBM MQ for z/OS .

Automatizujte zajišťování nebo zrušení zajišťování lokálních front IBM MQ a proveďte akce pro zajištěné fronty.

K dispozici jsou následující ukázkové sledy prací z/OSMF specifické pro frontu:

Název sledu prací	Popis
defineQueue.xml	Definovat lokální frontu Tento ukázkový sled prací demonstruje, jak lze sledy prací produktu z/OSMF použít k definování malých, středních nebo velkých front na základě nastavení vlastností. **Poznámka:** K dispozici je soubor typu manifest (`provision.mf`), který pomáhá s přidáním šablony pro tento sled prací. Tento soubor obsahuje odkaz na soubor **qaas_readme.pdf** , který obsahuje další informace. K souboru můžete přistupovat prostřednictvím odkazu po přidání šablony.
displayQueue.xml	Zobrazit vybrané atributy lokální fronty Tento ukázkový sled prací zobrazuje vybrané atributy lokální fronty. Atributy jsou vráceny v proměnné z/OSMF (název proměnné viz kroky ve sledu prací) a následně se zobrazí. V případě potřeby lze k obsahu proměnné přistupovat pomocí REST API. Další podrobnosti viz Rozhraní REST API zajišťování cloudua také viz z/OSMF služby sledu prací.
deleteQueue.xml	Odstranit lokální frontu Tento ukázkový sled prací odstraní lokální frontu v zadaném správci front.
putQueue.xml	Vložte jednu nebo více zpráv do lokální fronty. Tento ukázkový sled prací vloží jednu nebo více zpráv do lokální fronty. Text zprávy může být uveden, ale pokud je do lokální fronty současně vložena více než jedna zpráva, použije se stejný text zprávy.
getQueue.xml	Získat jednu nebo více zpráv z lokální fronty. Tento ukázkový sled prací získá jednu nebo více zpráv z lokální fronty. Zprávy jsou vráceny v proměnné z/OSMF (název proměnné viz kroky ve sledu prací) a následně se zobrazí. V případě potřeby můžete přistupovat k obsahu proměnné pomocí REST API. Další podrobnosti viz Rozhraní REST API zajišťování cloudua také viz z/OSMF služby sledu prací.
loadQueue.xml	Načíst zprávy z datové sady do lokální fronty. Tento ukázkový sled prací načítá zprávy z datové sady do lokální fronty. Výchozí název datové sady je určen nastavením vlastnosti. Další informace naleznete v tématu “Spuštění sledů prací” na stránce 1004.
offloadQueue.xml	Odlehčení zpráv z lokální fronty do datové sady.

Název sledu prací	Popis
	Tento ukázkový sled prací vyřadí zprávy z lokální fronty do datové sady. Výchozí název datové sady je určen nastavením vlastnosti. Další informace naleznete v tématu “Spuštění sledů prací” na stránce 1004.
clearQueue.xml	Vymazat zprávy v lokální frontě. Tento ukázkový sled prací vymaže (odstraní) všechny zprávy v lokální frontě.

Notes:

1. Akce **Vložit frontu** vám umožňuje zadat některá data zprávy a vložit jednu nebo více zpráv do fronty. Má-li být během daného požadavku do fronty umístěna více než jedna zpráva, použijí se stejná data zprávy.
2. Sledy prací loadQueue.xml a offloadQueue.xml vyvolávají spustitelný modul CSQUDMSG v knihovně SCSQLOAD s aliasem QLOAD. Jedná se o ekvivalent k obslužnému programu **dmpmqmsg** , který je k dispozici s produktem IBM MQ for Multiplatforms. Proto se očekává, že zprávy načtené z datové sady do fronty nebo z fronty do datové sady budou ve formátu **dmpmqmsg** .

   Ukázkový soubor JCL je také poskytován jako člen CSQ4QLOD v SCSQPROC.

   Nejjednodušší způsob, jak vyzkoušet akce loadQueue a offloadQueue , je provést následující:

   a. Zadejte **putQueue** několikrát pro vložení některých zpráv do fronty.

   b. **offloadQueue** slouží k odlehčení zpráv z fronty do datové sady.

   c. V případě potřeby odeberte všechny zprávy z fronty zadáním příkazu **clearQueue** .

   d. Pomocí funkce **loadQueue** načtěte zprávy z datové sady do stejné nebo jiné fronty.

   Máte-li zájem o formát **dmpmqmsg** , můžete procházet obsah datové sady po vydání požadavku na odlehčování.
3. Můžete provést akce **displayQueue**, **deleteQueue**, **putQueue**, **getQueue**, **loadQueue**, **offloadQueue**a **clearQueue** jako akce pro zajištěnou lokální frontu IBM MQ for z/OS . Další podrobnosti o akcích a souborech akcí naleznete v příručce *z/OSMF Programming Guide*.
4. Standardně se odstraní všechny sledy prací související s akcí. Důvodem je minimalizace potřeby uživatelů vyčistit sledy prací.

   Problém s tím však spočívá v tom, že akce vede k nějakému výstupu. Například akce **displayQueue** a **getQueue** vytvářejí výstup.

   Výstup nelze vidět, protože související sled prací je odstraněn, jakmile je akce provedena. Pokud tedy řídíte akce sledu prací z z/OS WUI, musíte nastavit příznak **cleanAfterComplete** na hodnotu *false* ve značce **< workflow>** pro každou akci, jejíž výstup chcete zobrazit.

   Chcete-li například zobrazit výstup souboru **displayQueue**, nastavte příznak následujícím způsobem:

```
<action name="displayQueue">
  <workflow cleanAfterComplete="false">
  ...

  ...
  </workflow>
</action>
```

   To však znamená, že musíte ručně vyčistit sledy prací související s akcemi.

Každý ukázkový sled prací z/OSMF provádí jeden nebo více kroků. Komentáře ve sledech prací vysvětlují funkci prováděnou jednotlivými kroky. Některé kroky pouze vyžadují datový vstup, zatímco některé kroky odesílají JCL a jiné vyvolávají spustitelné soubory REXX, aby splnily uvedenou funkci.

Přesný název souborů exec JCL nebo REXX naleznete v jednotlivých krocích. Sledy prací a přidružené soubory JCL nebo REXX exec odkazují na proměnné, které jsou deklarovány v jednom nebo více “Soubory deklarace proměnných sledu prací” na stránce 1004.

Související pojmy

“Omezení” na stránce 999
Omezení při použití z/OSMF s IBM MQ.

z/OS Spuštění sledů prací

Popis souborů, na které odkazuje ukázka sledů prací produktu z/OSMF , a způsob spuštění sledu prací.

Soubory deklarace proměnných sledu prací

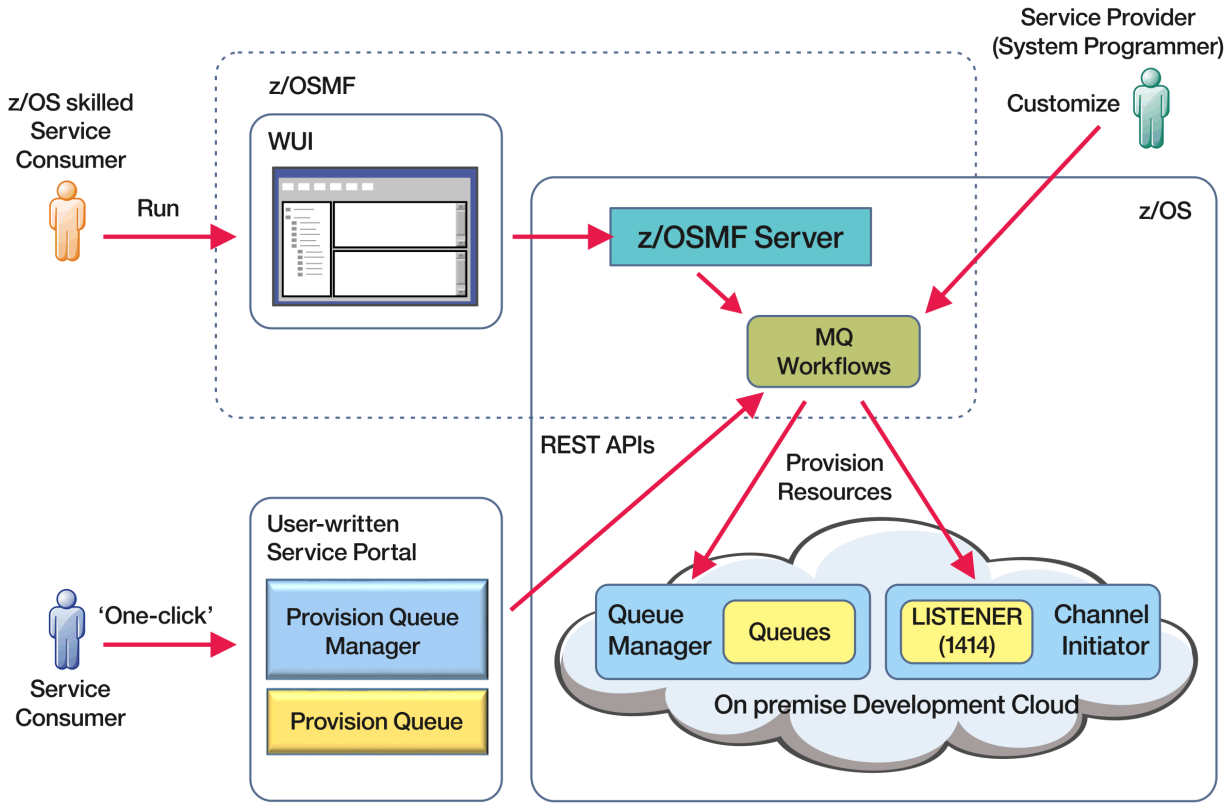
Následující soubory deklarují proměnné, na které odkazují ukázkové sledy prací z/OSMF a přidružené soubory JCL nebo REXX exec:

Název souboru deklarace proměnné sledu prací	Popis
common_variables.xml	Proměnné společné jak pro správce front (plus iniciátor kanálu), tak pro sledy prací fronty.
qmgr_variables.xml	Proměnné specifické pro sledy prací správce front (plus inicializátor kanálu).
queue_variables.xml	Proměnné specifické pro sledy prací fronty.
tcpip_variables.xml	Proměnné specifické pro sledy prací správce front (plus iniciátor kanálu) a používané pro identifikaci prostředků TCP/IP.

Poznámka: Výchozí viditelnost proměnných je *soukromá*. Chcete-li povolit dotazování na proměnné pomocí z/OSMF REST API, byly vybrané proměnné označeny jako *veřejné*. V případě potřeby však můžete změnit viditelnost dané proměnné.

Spuštění sledů prací

Obrázek 125. Zajišťování prostředků IBM MQ for z/OS jedním klepnutím



Před spuštěním sledů prací je třeba nastavit některé vlastnosti v následujícím souboru:

Název souboru vlastností proměnné sledu prací	**Popis**
workflow_variables.properties	Počáteční vlastnosti pro proměnné sledu prací. Komentáře v souboru uvádějí účel každé vlastnosti. • Vlastnosti v metazávorkách (< >) musí být nastaveny na hodnoty specifické pro uživatele. • Vlastnost prostředí lze nastavit tak, aby zajišťovala správce front pro vývojová (DEV), testovací (TEST), zajištění kvality (QA) nebo produkční (PROD) prostředí. Další nastavení vlastností řídí charakteristiky správce front, který má být zajišťován pro každé prostředí. Můžete například změnit počet aktivních protokolů nebo počet sad stránek pro každý typ prostředí. • Ostatní vlastnosti jsou nastaveny na výchozí hodnoty IBM MQ , ale v případě potřeby je lze upravit tak, aby splňovaly lokální konvence.

Obecně platí, že po nastavení vlastností lze sledy prací spouštět tak, jak jsou. V případě potřeby však můžete upravit sled prací a upravit nebo odebrat existující kroky nebo přidat nové kroky.

Sledy prací lze spustit:

- Z rozhraní z/OSMF WUI.

  Z nabídky Cloud Provisioning-> Softwarové služby ve WUI lze sledy prací spustit v automatickém nebo ručním režimu. Ruční režim je užitečný při testování a v obou režimech lze sledovat průběh jednotlivých kroků sledu prací.

  Další podrobnosti viz Služby zajišťování cloudu a Vytvořit sled prací.

- Použití služeb z/OSMF REST Workflow Services.

  Služby REST Workflow Services lze použít ke spouštění sledů prací prostřednictvím REST API. Tento režim je užitečný pro vytváření operací jednoho klepnutí z portálu napsaného uživatelem.

  Další podrobnosti viz Rozhraní REST API zajišťování cloudua také viz z/OSMF služby sledu prací.
- Použití ukázkového portálu tržiště, který je poskytován s produktem z/OSMF.

Související pojmy

“Automatizace zajišťování objektů IBM MQ” na stránce 1001

Ukázky jsou dodávány pro automatizaci zajišťování správců front a lokálních front.

z/OS MQ Adv. VUE Povolení konektivity agenta MFT ke vzdáleným z/OS správcům front

V některých případech se Managed File Transfer agenti v systému z/OS mohou připojit ke vzdálenému správci front v systému z/OS pomocí připojení klienta. To může vést k jednodušším IBM MQ topologiím.

Klientská připojení ke vzdáleným správcům front z/OS jsou podporována v následujících případech:

- LTS V 9.3.4 Agent MFT je IBM MQ 9.3.4 nebo novější, nebo Long Term Support s použitou opravou APAR PH56722 a byl přidružen k identifikátoru produktu (PID) buď IBM MQ Advanced for z/OS VUE, nebo IBM MQ Advanced for z/OS.
- Agent MFT je na adrese IBM MQ 9.3.0 a byl přidružen k PID IBM MQ Advanced for z/OS VUE.

Informace o různých PID viz IBM MQ identifikátory produktu a informace o exportu .

Informace o nastavení PID přidruženého k instalaci produktu MFT naleznete v tématu **`fteSetProductId`** .

PID, pod kterým je agent spuštěn, se zobrazí v protokolu při spuštění agenta.

Agent MFT v systému z/OSspuštěný pod jakýmkoli jiným PID se může připojit pouze k lokálnímu správci front pomocí připojení v režimu vazeb.

Pokud se agent pokusí připojit ke správci front, který není spuštěn v systému z/OS, je vydána zpráva BFGQM1044E a spuštění agenta je ukončeno.

Související úlohy

Spuštění agenta MFT v systému z/OS

Konfigurace produktu IBM MQ Internet Pass-Thru

Tento oddíl popisuje různé funkce, které produkt IBM MQ Internet Pass-Thru (MQIPT) podporuje, a jak je konfigurovat.

Nakonfigurujte MQIPT provedením změn v konfiguračním souboru `mqipt.conf`. Struktura konfiguračního souboru MQIPT a vlastnosti, které lze zadat, jsou popsány v tématu IBM MQ Internet Pass-Thru odkaz na konfiguraci.

Poznámka: Měli byste nastavit oprávnění k zabezpečeným souborům v adresáři, kde je umístěn soubor `mqipt.conf` , abyste zabránili neoprávněným uživatelům zobrazit jakákoli uložená hesla nebo změnit konfiguraci. Ochraňte všechna hesla uvedená v konfiguračním souboru podle procedury uvedené v části “Šifrování uložených hesel v adresáři MQIPT” na stránce 1046.

Změny konfiguračního souboru se projeví po spuštění nebo aktualizaci souboru MQIPT . Aktualizace aktivní instance produktu MQIPT uvede změny konfigurace v platnost bez restartování MQIPT. Když se aktualizuje soubor MQIPT , konfigurační soubor `mqipt.conf` se znovu přečte a produkt MQIPT provede následující akce:

- Všechny aktivní trasy, které jsou označeny jako neaktivní nebo již nejsou uvedeny v konfiguračním souboru, jsou uzavřeny a již nepřijímají příchozí připojení.

- Všechny trasy, které jsou v konfiguračním souboru označeny jako aktivní a nejsou momentálně spuštěny, jsou spuštěny.
- Všechny změny konfiguračních parametrů aktivních přenosových cest se použijí. Pokud je to možné, tyto změny se projeví bez narušení aktivních připojení. U některých změn parametrů, jako např. změna místa určení přenosové cesty, jsou všechna připojení uzavřena před použitím změny a restartováním přenosové cesty.

Chcete-li aktualizovat soubor MQIPT, použijte příkaz **mqiptAdmin** . Další informace o administraci produktu MQIPT pomocí příkazu **mqiptAdmin** naleznete v tématu Administrace MQIPT pomocí příkazového řádku.

HTTP v MQIPT

MQIPT podporuje tunelové propojení HTTP . MQIPT lze konfigurovat tak, aby datové pakety, které předává, byly kódovány jako požadavky HTTP .

Kanály IBM MQ nepřijímají požadavky HTTP . Proto je pro přijetí požadavků HTTP a jejich převedení zpět na pakety protokolu IBM MQ vyžadována druhá hodnota MQIPT . Druhý MQIPT odebere záhlaví HTTP pro převod příchozího paketu zpět na standardní paket protokolu IBM MQ před jeho předáním správci cílové fronty.

Při použití protokolu HTTP mezi dvěma instancemi produktu MQIPTje připojení TCP/IP, ve kterém jsou požadavky a odpovědi HTTP trvalé a jsou uchovány otevřené po dobu životnosti kanálu zpráv. MQIPT nezavírá spojení TCP/IP mezi dvojicemi požadavek/odpověď.

Pokud dvě instance produktu MQIPT komunikují prostřednictvím HTTP, je možné, že požadavek HTTP zůstane nevyřízený po delší dobu. Příklad je v kanálu žadatele/serveru, když strana serveru čeká na příchod nových zpráv do své přenosové fronty. Protokol kanálu IBM MQ poskytujemechanismus "prezenčního signálu", který vyžaduje, aby čekací konec pravidelně odesílal zprávy prezenčního signálu svému partnerovi. Výchozí doba prezenčního signálu kanálu je 5 minut. Produkt MQIPT používá tento prezenční signál jako odpověď HTTP . Nezakazujte tento prezenční signál kanálu ani jej nenastavujte na příliš vysokou hodnotu, abyste se vyhnuli problémům s vypršením časového limitu v některých branách firewall.

MQIPT přijímá provoz HTTP v chunked formátu, generovaný serverem proxy nebo serverem HTTP .

Příklad použití HTTP v souboru MQIPTnaleznete v tématu Konfigurace HTTP tunelového propojení.

HTTP proxy

Server proxy HTTP lze umístit mezi dvě instance produktu MQIPT. Server proxy HTTP musí splňovat následující požadavky:

- Server proxy musí podporovat protokol HTTP 1.1 .
- Záhlaví **Connection** nebo **Proxy-Connection** HTTP , která jsou nastavena pomocí MQIPT , musí být uznána serverem proxy. To umožňuje, aby byla připojení mezi dvěma instancemi produktu MQIPT ponechána otevřená po dobu životnosti kanálu zpráv.
- V rámci serveru proxy musí být udržováno mapování trvalých připojení jedna ku jedné. Tím se zajistí, že připojení TCP/IP ze serveru proxy k místu určení MQIPT nebudou použita k přenosu dat pro více než jeden kanál zpráv.

Můžete nastavit vlastnosti pro konfiguraci způsobu správy trvalých připojení na některých serverech proxy HTTP . Můžete například nastavit maximální počet požadavků, které lze provést na trvalém připojení. Měly by být nastaveny následující vlastnosti:

- Trvalá připojení by měla být povolena.
- Opětovné použití připojení TCP/IP ze serveru proxy do produktu MQIPT více než jednou relací HTTP by mělo být zakázáno, aby se zachovalo mapování trvalých připojení přes server proxy jedna ku jedné.
- Časový limit pro požadavky serveru proxy by měl být nastaven na vysokou hodnotu. Například 12 hodin.

- Maximální počet požadavků, které lze provést na trvalém připojení, by měl být nastaven na vysokou hodnotu. Například 5000.

Produkt MQIPT používá požadavky POST HTTP k odesílání dat mezi dvěma instancemi produktu MQIPT. Pokud konfigurace MQIPT určuje název hostitele serveru proxy pomocí vlastnosti **HTTPProxy** , produkt MQIPT se připojí k serveru proxy a použije metodu HTTP CONNECT k požadavku, aby server proxy vytvořil tunel k místu určení MQIPT. To umožňuje připojení HTTPS projít přes server proxy bez ukončení relace TLS v serveru proxy.

Pokud je prostředek pro vyrovnávání zátěže umístěn mezi instancemi MQIPT , musí být nakonfigurován tak, aby používal hodnotu souboru cookie *MQIPTSessionId* HTTP , aby se zajistilo, že všechny požadavky pro každou relaci budou předány do stejného místa určení.

HTTPS v MQIPT

HTTPS lze použít pro připojení HTTP povolením vlastností směrování **HTTPS** a **SSLClient** na serveru MQIPT , který vydává připojení klienta.

Produkt MQIPT musí mít přístup k důvěryhodnému certifikátu CA, který bude použit k ověření cílového serveru proxy HTTP . Vlastnost **SSLClientCAKeyring** lze použít k definování souboru svazku klíčů obsahujícího důvěryhodný certifikát CA.

Společné nastavení pro HTTPS bude používat lokální server proxy HTTP pro tunelové propojení přes bránu firewall a připojení ke vzdálenému serveru HTTP (nebo jinému serveru proxy), který se následně připojí ke vzdálenému serveru MQIPT. Tento MQIPT na straně serveru připojení nepotřebuje žádnou specifickou konfiguraci, protože požadavek na připojení je považován za normální připojení HTTP .

Produkt MQIPT používá vlastnosti **HTTPProxy** a **HTTPServer** k rozlišení lokálních a vzdálených serverů proxy. Trasa MQIPT se sadou vlastností **HTTPProxy** je považována za lokální server proxy HTTP a trasa MQIPT se sadou vlastností **HTTPServer** je vzdálený server (nebo server proxy).

HTTPS se obvykle provádějí na adrese portu modulu listener 443 na serveru proxy HTTP , ale vlastnosti **HTTPProxyPort** a **HTTPServerPort** lze použít k přepsání této výchozí hodnoty.

Podpora SOCKS v MQIPT

Server proxy SOCKS je síťová služba používaná jako řízený bod ukončení přes bránu firewall. Aplikace s podporou SOCKS, která běží uvnitř brány firewall, může použít server proxy SOCKS pro připojení ke vzdálené aplikaci.

Produkt MQIPT může fungovat jako server proxy SOCKS tak, že povolí vlastnost **SocksServer** , čímž umožní aplikaci IBM MQ s povoleným SOCKS připojit se prostřednictvím produktu MQIPT ke vzdálenému správci front IBM MQ . Při použití této funkce jsou cílový cíl a adresa cílového portu získány během procesu navázání komunikace SOCKS, a proto jsou vlastnosti směrování **Destination** a **DestinationPort** přepsány. Jedná se o klíčovou funkci pro podporu klastrování produktu IBM MQ .

Produkt MQIPT může také vystupovat jako klient SOCKS jménem lokální aplikace IBM MQ , která nebyla povolena. To je užitečné při použití brány firewall, která umožňuje odchozí připojení pouze prostřednictvím serveru proxy SOCKS. Každou trasu MQIPT lze nakonfigurovat tak, aby komunikovala s jiným serverem proxy SOCKS.

Příklad použití SOCKS viz Konfigurace serveru proxy SOCKS .

Klastrování v produktu MQIPT

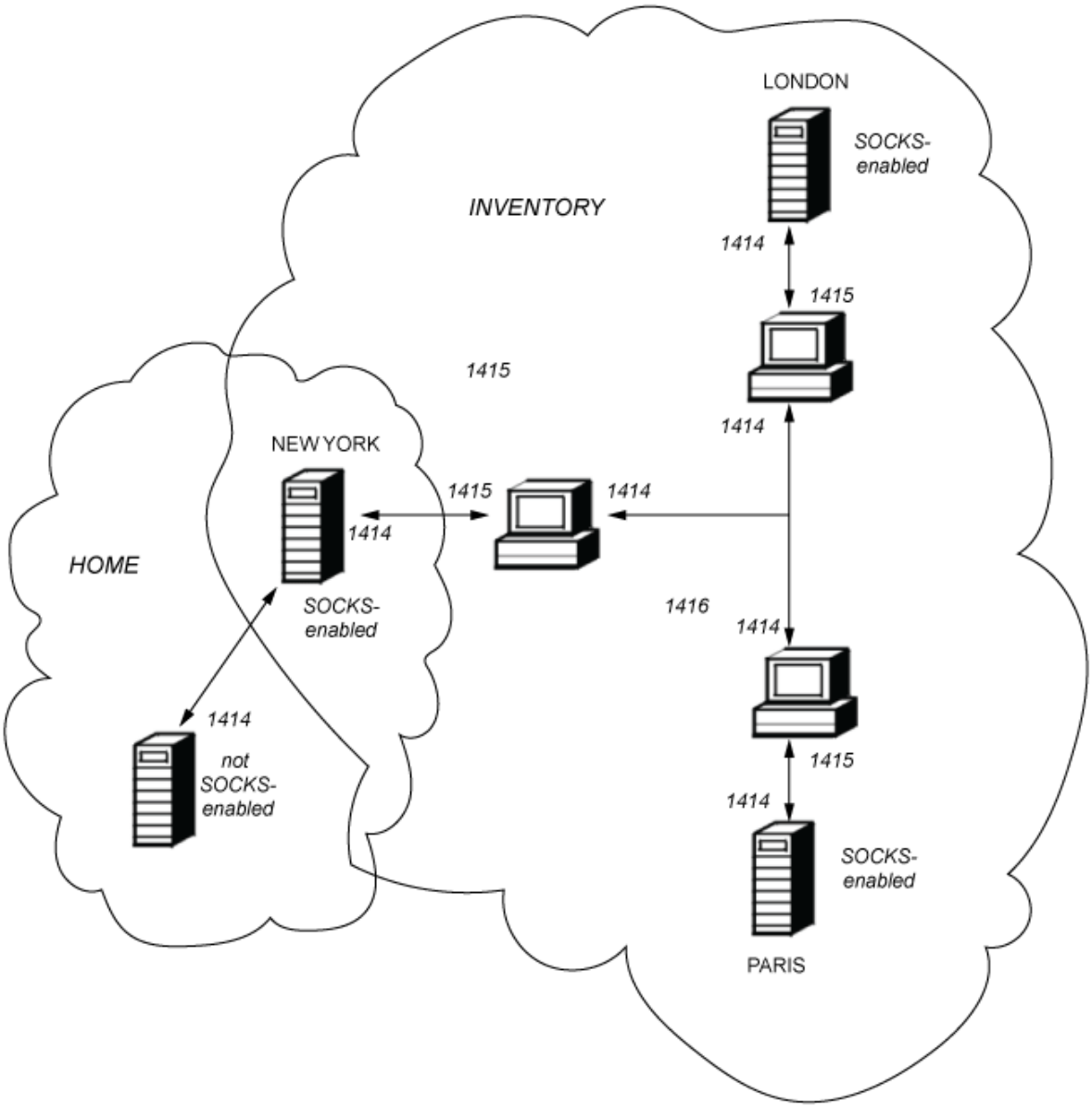
Klastry IBM MQ mohou být použity s produktem MQIPT pomocí SOCKS-povolení všech správců front v klastru, který se nachází na Internetu, a povolení produktu MQIPT , aby vystupovala jako server proxy SOCKS.

V následujícím diagramu jsou NEWYORK a CHICAGO v klastru s názvem HOME a obě obsahují úplná úložiště. NEWYORK, LONDON a PARIS jsou v jiném klastru nazvaném INVENTORY. Všimněte si, že CHICAGO nemusí mít povolen SOCKS, protože je v klastru, který nepotřebuje MQIPT.

Každý správce front v klastru INVENTORY je účinně "skrytý" za položkou MQIPT. Vzhledem k tomu, že pro správce front byla povolena volba SOCKS, je při spuštění odesílacího kanálu klastru odeslán požadavek do místa určení s použitím produktu MQIPT , který funguje jako server proxy SOCKS. Obvykle se název CONNAME v přijímacím kanálu klastru používá k identifikaci lokálního správce front, ale při použití s produktem MQIPTmusí název CONNAME identifikovat lokální MQIPT a jeho příchozí port modulu listener. V následujícím diagramu jsou všechny příchozí adresy portů modulu listener 1414 a odchozí adresy portů modulu listener 1415.

Existují dva způsoby spuštění správce front s podporou SOCKS. První je SOCKS-povolte celý počítač, kde je spuštěn správce front. Druhým je SOCKS-povolit pouze správce front. Pomocí jedné z těchto metod musíte nakonfigurovat klienta SOCKS tak, aby vytvářoval pouze vzdálená připojení používající server proxy MQIPT jako server proxy SOCKS a zakázal ověřování uživatelů. Existuje celá řada produktů na trhu k dosažení podpory SOCKS. Musíte vybrat ten, který podporuje protokol SOCKS V5 .

Příklad konfigurace sítě klastru naleznete v tématu Konfigurace MQIPT podpory klastrování .



Podpora SSL/TLS v souboru MQIPT

Zabezpečené sokety lze použít k zajištění soukromí komunikace, integrity komunikace a ověření.

Ochrana osobních údajů
Připojení lze nastavit jako soukromé. Data, která mají být vyměněna mezi klientem a serverem, mohou být šifrována a pouze odesílatel a příjemce mohou mít smysl pro data. To znamená, že soukromé informace, například čísla kreditních karet, mohou být bezpečně přeneseny.

Integrita komunikace
Připojení je spolehlivé. Přenos zpráv zahrnuje kontrolu integrity zpráv na základě zabezpečené hašovací funkce.

Ověřování
Klient může ověřit server a ověřený server může ověřit klienta. To znamená, že je zaručeno, že informace budou vyměňovány pouze mezi zamýšlenými stranami. Mechanismus ověřování je založen na výměně digitálních certifikátů (certifikátyX.509v3).

Protokoly zabezpečených soketů

V produktu MQIPTjsou zabezpečené sokety poskytovány pomocí protokolů TLS (Transport Layer Security) a SSL (Secure Sockets Layer). Dva protokoly zabezpečených soketů jsou podobné, ale nespolupracují. V této dokumentaci se výrazy SSL a TLS používají zaměnitelně, pokud není zaznamenán specifický rozdíl.

Produkt MQIPT podporuje zabezpečení SSL 3.0, TLS 1.0, TLS 1.1a TLS 1.2 poskytované dodaným prostředím Java runtime environment (JRE). V 9.3.0 Od verze IBM MQ 9.3.0produkt MQIPT také podporuje protokol TLS 1.3. IBM MQ CipherSpec vzdáleného kanálu určuje, který protokol MQIPT používá.

Zabezpečení SSL 3.0, TLS 1.0a TLS 1.1 jsou nezabezpečené a ve výchozím nastavení jsou v produktu MQIPTzakázány. Potřebujete-li použít některý z těchto zakázaných protokolů, můžete je znovu povolit pomocí postupu uvedeného v části “Povolení zamítnutých protokolů a sad šifrování v produktu MQIPT” na stránce 1034.

Protokoly SSL/TLS mohou používat různé algoritmy digitálního podpisu pro ověřování komunikačních stran. Šifrovací operace, které se používají v SSL/TLS, šifrování pro utajení dat a zabezpečené hašování pro integritu zpráv, spoléhají na sdílení tajných klíčů mezi klientem a serverem. SSL/TLS poskytuje různé mechanismy výměny klíčů, které umožňují sdílení tajných klíčů. SSL/TLS může využívat různé algoritmy pro šifrování a hašování.

Povolení režimu FIPS v MQIPT

Šifrovací komponenta SSL/TLS prostředí JRE obsahuje poskytovatele zabezpečení `IBMJCEPlusFIPS` , který je certifikován v souladu se standardem FIPS 140-2. Chcete-li v produktu MQIPTpoužívat pouze šifrování s certifikací FIPS, povolte režim FIPS v poskytovateli `IBMJSSE2` nastavením následujících systémových vlastností Java při spuštění produktu MQIPT :

- `com.ibm.jsse2.usefipsprovider=true`
- V 9.3.0 `com.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS`

Vlastnosti systému Java můžete nastavit při spuštění produktu MQIPT pomocí proměnné prostředí **`MQIPT_JVM_OPTIONS`** . Například v systému Linuxzadejte následující příkaz k nastavení proměnné prostředí před zadáním příkazu ke spuštění MQIPT:

```
export MQIPT_JVM_OPTIONS="-Dcom.ibm.jsse2.usefipsprovider=true
-Dcom.ibm.jsse2.usefipsProviderName=IBMJCEPlusFIPS"
```

Další informace o povolení režimu FIPS naleznete v tématu Povolení režimu FIPS v poskytovateli IBMJSSE2.

Režim přemostění SSL/TLS

Je-li pro trasu nastaven SSLServer i SSLClient, produkt MQIPT přijme jedno příchozí zabezpečené připojení SSL/TLS a vytvoří druhé zabezpečené připojení SSL/TLS k jinému MQIPT nebo ke správci cílové fronty. Informace kanálu IBM MQ jsou dešifrovány a znovu šifrovány mezi těmito dvěma připojeními SSL/TLS. Přemostění SSL/TLS se také označuje jako *proxy pro ukončení SSL/TLS*.

Produkt IBM MQ podporuje přemostění SSL/TLS pomocí MQIPT. Bylo zjištěno, že jiné servery proxy pro ukončení SSL/TLS s produktem IBM MQ způsobují nefunkční připojení, pokud server proxy kombinuje nebo rekonstruuje záznamy SSL/TLS s jinou velikostí než ty, které odeslal produkt IBM MQ. Důvodem je interakce mezi způsobem, jakým správci front přidělují a spravují paměť pro příchozí síťová data systému IBM MQ a způsobem, jakým jsou síťová data systému IBM MQ zabalena do záznamů SSL/TLS.

Produkt MQIPT zachovává balení síťových dat IBM MQ v záznamech SSL/TLS, aniž by je rozděloval nebo kombinoval. Pokud jiné mosty SSL/TLS neuchovávají záznamy SSL/TLS přesně, mohou způsobit, že kanály IBM MQ selžou s chybovými zprávami:

```
AMQ9638: SSL communications error for channel
AMQ9208: Error on receive from host
```

Režim serveru proxy SSL/TLS

Přenosovou cestu MQIPT lze konfigurovat v režimu serveru proxy SSL/TLS jako alternativu k přemostění SSL/TLS. V tomto režimu přenosová cesta pouze předává data SSL/TLS mezi dvěma koncovými body IBM MQ ; neúčastní se navázání komunikace SSL/TLS a nevyžaduje žádné digitální certifikáty.

Režim serveru proxy SSL/TLS můžete použít v případech, kdy jsou kanály IBM MQ , které komunikují prostřednictvím produktu MQIPT , již konfigurovány pro komunikaci SSL/TLS a chcete použít produkt MQIPT pro jiný účel, například směrování připojení přes brány firewall nebo omezení sady povolených připojení prostřednictvím uživatelské procedury zabezpečení. Při spuštění v režimu serveru proxy SSL/TLS produkt MQIPT zkontroluje, zda jsou počáteční pakety SSL/TLS přijaté z nového připojení platné před postoupením paketů do cíle.

Produkt IBM MQ podporuje režim serveru proxy SSL/TLS s produktem MQIPT nebo jakýmkoli jiným serverem proxy SSL/TLS.

IBM MQ podpora více certifikátů s MQIPT

Produkt IBM MQ 8.0a novější podporují použití více certifikátů ve stejném správci front s použitím popisku certifikátu pro jednotlivé kanály určeného pomocí atributu **CERTLABL** v definici kanálu. Příchozí kanály do správce front (například připojení k serveru nebo příjemce) spoléhají na zjištění názvu kanálu pomocí SNI (TLS Server Name Indication), aby bylo možné předložit správný certifikát ze správce front. Další informace o použití více certifikátů ve správci front naleznete v tématu Jak produkt IBM MQ poskytuje možnost použití více certifikátů.

Pokud se kanál připojuje ke správci cílové fronty prostřednictvím produktu MQIPTa pro trasu MQIPT jsou nastaveny hodnoty **SSLServer** i **SSLClient** , existují mezi koncovými body dvě samostatné relace TLS. Ve verzích starších než IBM MQ 9.3.0data SNI netečou přes přerušení relace. Tím zabráníte použití certifikátu pro jednotlivé kanály ve správci cílové fronty pro připojení TLS mezi produktem MQIPT a správcem front. Chcete-li použít certifikát pro každý kanál ve správci cílové fronty, musí pro připojení TLS, které prochází produktem MQIPT ve verzi dřívější než IBM MQ 9.3.0, směrování MQIPT používat režim serveru proxy SSL/TLS, který předá všechny řídicí toky TLS neporušené, včetně názvu SNI.

V 9.3.0 Od IBM MQ 9.3.0lze MQIPT konfigurovat pomocí vlastnosti směrování SSLClientOutboundSNI buď nastavit SNI pro připojení TLS na specifickou hodnotu, nebo projít SNI přijatou při příchozím připojení k přenosové cestě. Chcete-li povolit použití certifikátů pro jednotlivé kanály ve správci cílové fronty, musí být přenosová cesta buď konfigurována tak, aby nastavila SNI na název kanálu IBM MQ , nebo aby prošla přes SNI přijaté v příchozím připojení k přenosové cestě. Je-li produkt MQIPT konfigurován pro průchod přes rozhraní SNI, musí správce front nebo klient, který se připojuje k produktu MQIPT , nastavit rozhraní SNI na název kanálu.

Certifikáty, které se používají pro připojení TLS ukončená nebo zahájená produktem MQIPT , lze konfigurovat jednotlivě pro každou trasu, například pomocí vlastností trasy **SSLServerSiteLabel** a **SSLClientSiteLabel** .

CipherSuites podporované MQIPT

Následující tabulka zobrazuje, které sady CipherSuites jsou podporovány produktem MQIPT a které jsou standardně povoleny.

Standardně je povolena pouze podmnožina CipherSuites . CipherSuites založené na několika algoritmech, které jsou považovány za nezabezpečené, jsou prostředím JRE zakázány. Pokud jste si vědomi potenciálních rizik, ale stále potřebujete použít jednu z těchto CipherSuites, můžete přidat podporu pro zakázanou CipherSuite podle postupu v části "Povolení zamítnutých protokolů a sad šifrování v produktu MQIPT" na stránce 1034.

Tabulka 70. CipherSuites , které můžete používat s produktem MQIPT .

CipherSuite	**Standardně povoleno**
CipherSuites pro protokol TLS 1.3	
V 9.3.0 V 9.3.0 TLS_AES_128_GCM_SHA256	Ano
V 9.3.0 V 9.3.0 TLS_AES_256_GCM_SHA384	Ano
V 9.3.0 V 9.3.0 TLS_CHACHA20_POLY1305_SHA256	Ano
CipherSuites pro zabezpečení SSL 3.0, TLS 1.0, TLS 1.1 a TLS 1.2	
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	
SSL_DH_anon_WITH_AES_128_CBC_SHA	
SSL_DH_anon_WITH_AES_128_CBC_SHA256	
SSL_DH_anon_WITH_AES_128_GCM_SHA256	
SSL_DH_anon_WITH_AES_256_CBC_SHA	
SSL_DH_anon_WITH_AES_256_CBC_SHA256	
SSL_DH_anon_WITH_AES_256_GCM_SHA384	
SSL_DH_anon_WITH_DES_CBC_SHA	
SSL_DH_anon_WITH_RC4_128_MD5	
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	
SSL_DHE_DSS_WITH_AES_128_CBC_SHA	Ano
SSL_DHE_DSS_WITH_AES_128_CBC_SHA256	Ano
SSL_DHE_DSS_WITH_AES_128_GCM_SHA256	Ano
SSL_DHE_DSS_WITH_AES_256_CBC_SHA	Ano
SSL_DHE_DSS_WITH_AES_256_CBC_SHA256	Ano
SSL_DHE_DSS_WITH_AES_256_GCM_SHA384	Ano

Tabulka 70. CipherSuites , které můžete používat s produktem MQIPT . (pokračování)	
CipherSuite	**Standardně povoleno**
SSL_DHE_DSS_WITH_DES_CBC_SHA	
SSL_DHE_DSS_WITH_RC4_128_SHA	
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_DHE_RSA_WITH_AES_128_CBC_SHA	Ano
SSL_DHE_RSA_WITH_AES_128_CBC_SHA256	Ano
SSL_DHE_RSA_WITH_AES_128_GCM_SHA256	Ano
SSL_DHE_RSA_WITH_AES_256_CBC_SHA	Ano
SSL_DHE_RSA_WITH_AES_256_CBC_SHA256	Ano
SSL_DHE_RSA_WITH_AES_256_GCM_SHA384	Ano
SSL_DHE_RSA_WITH_DES_CBC_SHA	
SSL_ECDH_anon_WITH_3DES_EDE_CBC_SHA	
SSL_ECDH_anon_WITH_AES_128_CBC_SHA	
SSL_ECDH_anon_WITH_AES_256_CBC_SHA	
SSL_ECDH_anon_WITH_NULL_SHA	
SSL_ECDH_anon_WITH_RC4_128_SHA	
SSL_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Ano
SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	Ano
SSL_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	Ano
SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Ano
SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	Ano
SSL_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	Ano
SSL_ECDH_ECDSA_WITH_NULL_SHA	
SSL_ECDH_ECDSA_WITH_RC4_128_SHA	
SSL_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDH_RSA_WITH_AES_128_CBC_SHA	Ano
SSL_ECDH_RSA_WITH_AES_128_CBC_SHA256	Ano
SSL_ECDH_RSA_WITH_AES_128_GCM_SHA256	Ano
SSL_ECDH_RSA_WITH_AES_256_CBC_SHA	Ano
SSL_ECDH_RSA_WITH_AES_256_CBC_SHA384	Ano
SSL_ECDH_RSA_WITH_AES_256_GCM_SHA384	Ano
SSL_ECDH_RSA_WITH_NULL_SHA	
SSL_ECDH_RSA_WITH_RC4_128_SHA	

Tabulka 70. CipherSuites , které můžete používat s produktem MQIPT . (pokračování)	
CipherSuite	**Standardně povoleno**
SSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Ano
SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Ano
SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Ano
SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Ano
SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Ano
SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Ano
SSL_ECDHE_ECDSA_WITH_NULL_SHA	
SSL_ECDHE_ECDSA_WITH_RC4_128_SHA	
SSL_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA	Ano
SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Ano
SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Ano
SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA	Ano
SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Ano
SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Ano
SSL_ECDHE_RSA_WITH_NULL_SHA	
SSL_ECDHE_RSA_WITH_RC4_128_SHA	
SSL_KRB5_EXPORT_WITH_DES_CBC_40_MD5	
SSL_KRB5_EXPORT_WITH_DES_CBC_40_SHA	
SSL_KRB5_EXPORT_WITH_RC4_40_MD5	
SSL_KRB5_EXPORT_WITH_RC4_40_SHA	
SSL_KRB5_WITH_3DES_EDE_CBC_MD5	
SSL_KRB5_WITH_3DES_EDE_CBC_SHA	
SSL_KRB5_WITH_DES_CBC_MD5	
SSL_KRB5_WITH_DES_CBC_SHA	
SSL_KRB5_WITH_RC4_128_MD5	
SSL_KRB5_WITH_RC4_128_SHA	
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	
SSL_RSA_EXPORT_WITH_RC4_40_MD5	
SSL_RSA_WITH_3DES_EDE_CBC_SHA	
SSL_RSA_WITH_AES_128_CBC_SHA	Ano
SSL_RSA_WITH_AES_128_CBC_SHA256	Ano
SSL_RSA_WITH_AES_128_GCM_SHA256	Ano

Tabulka 70. CipherSuites , které můžete používat s produktem MQIPT . (pokračování)	
CipherSuite	**Standardně povoleno**
SSL_RSA_WITH_AES_256_CBC_SHA	Ano
SSL_RSA_WITH_AES_256_CBC_SHA256	Ano
SSL_RSA_WITH_AES_256_GCM_SHA384	Ano
SSL_RSA_WITH_DES_CBC_SHA	
SSL_RSA_WITH_NULL_MD5	
SSL_RSA_WITH_NULL_SHA	
SSL_RSA_WITH_NULL_SHA256	
SSL_RSA_WITH_RC4_128_MD5	Ano
SSL_RSA_WITH_RC4_128_SHA	
V 9.3.0 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	
V 9.3.0 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	
V 9.3.0 TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	

CipherSpecs a MQIPT CipherSuites

Následující tabulka zobrazuje vztah mezi specifikacemi CipherSpecs podporovanými produktem IBM MQ a CipherSuites podporovanými produktem MQIPT.

Tabulka také zobrazuje verzi protokolu, která IBM MQ očekává použití jednotlivých CipherSpec .

IBM MQ CipherSpec jedinečně určuje šifrovací algoritmus i verzi protokolu zabezpečeného soketu, která má být použita. Některé specifikace IBM MQ CipherSpecs se liší pouze podle verze protokolu, takže nestačí nakonfigurovat samotnou sadu CipherSuite . Navázání komunikace SSL/TLS vyjedná nejvyšší verzi protokolu zabezpečených soketů podporovanou oběma stranami a poté vybere CipherSuite ze sady vzájemně povolených šifer.

Například přenosová cesta SSLClient s `SSLClientCipherSuites=SSL_RSA_WITH_3DES_EDE_CBC_SHA` by mohla vyjednávat buď TLS_RSA_WITH_3DES_EDE_CBC_SHA (TLS 1.0), nebo TRIPLE_DES_SHA_US (SSL 3.0) se vzdáleným správcem front. Ve skutečnosti je možné vyjednávat tuto CipherSuite přes TLS 1.2, ale produkt IBM MQ nepodporuje tuto CipherSuite přes TLS 1.2. Z tohoto důvodu je zvláště pravděpodobné, že trasy SSLClient způsobí ve správci front chyby AMQ9616 nebo AMQ9631 .

Chcete-li se vyhnout takovým chybám na trasách SSLClient, nastavte vlastnost směrování **`SSLClientProtocols`** na odpovídající hodnotu pro zamýšlenou CipherSpec. V některých případech může být také nezbytné omezit sadu protokolů na straně serveru pomocí vlastnosti směrování **`SSLServerProtocols`** . Pomocí verze protokolu zobrazené v tabulce určete správné nastavení pro tyto vlastnosti trasy.

Tento problém se týká zejména následujících CipherSuites a CipherSpecs pro trasy SSLClient:

- SSL_RSA_WITH_3DES_EDE_CBC_SHA, což odpovídá:
  - SSL 3.0: MQ CipherSpec TRIPLE_DES_SHA_US
  - TLS 1.0: MQ CipherSpec TLS_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA, který odpovídá:
  - SSL 3.0: MQ CipherSpec DES_SHA_EXPORT

  - TLS 1.0: MQ CipherSpec TLS_RSA_WITH_DES_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA, což odpovídá:
  - SSL 3.0: MQ CipherSpec RC4_SHA_US
  - TLS 1.2: MQ CipherSpec TLS_RSA_WITH_RC4_128_SHA256

Chcete-li použít jednu trasu MQIPT SSLClient k tunelu pro více kanálů IBM MQ , které používají různé specifikace CipherSpecs, ujistěte se, že všechny kanály mají specifikace CipherSpecs , které používají stejnou verzi protokolu zabezpečených soketů jako ostatní, a že jste nastavili produkt **SSLClientProtocols** , aby používal tuto verzi jediného protokolu.

Další informace o specifikacích IBM MQ CipherSpecsnaleznete v tématu Povolení CipherSpecs.

IBM MQ CipherSpec	**MQIPT CipherSuite**	**Verze protokolu**
DES_SHA_EXPORT	SSL_RSA_WITH_DES_CBC_SHA	SSLv3
DES_SHA_EXPORT1024	Není k dispozici	Není k dispozici
ECDHE_ECDSA_3DES_EDE_CBC_SHA256	SSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.2
ECDHE_ECDSA_AES_128_CBC_SHA256	SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
ECDHE_ECDSA_AES_128_GCM_SHA256	SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
ECDHE_ECDSA_AES_256_CBC_SHA384	SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
ECDHE_ECDSA_AES_256_GCM_SHA384	SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
ECDHE_ECDSA_NULL_SHA256	SSL_ECDHE_ECDSA_WITH_NULL_SHA	TLSv1.2
ECDHE_ECDSA_RC4_128_SHA256	SSL_ECDHE_ECDSA_WITH_RC4_128_SHA	TLSv1.2
ECDHE_RSA_3DES_EDE_CBC_SHA256	SSL_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.2
ECDHE_RSA_AES_128_CBC_SHA256	SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
ECDHE_RSA_AES_128_GCM_SHA256	SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
ECDHE_RSA_AES_256_CBC_SHA384	SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
ECDHE_RSA_AES_256_GCM_SHA384	SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
ECDHE_RSA_NULL_SHA256	SSL_ECDHE_RSA_WITH_NULL_SHA	TLSv1.2
ECDHE_RSA_RC4_128_SHA256	SSL_ECDHE_RSA_WITH_RC4_128_SHA	TLSv1.2
NULL_MD5	SSL_RSA_WITH_NULL_MD5	SSLv3
NULL_SHA	SSL_RSA_WITH_NULL_SHA	SSLv3
RC2_MD5_EXPORT	Není k dispozici	Není k dispozici
RC4_56_SHA_EXPORT1024	Není k dispozici	Není k dispozici

IBM MQ CipherSpec	MQIPT CipherSuite	Verze protokolu
RC4_MD5_EXPORT	SSL_RSA_EXPORT_WITH_RC4_40_MD5	SSLv3
RC4_MD5_US	SSL_RSA_WITH_RC4_128_MD5	SSLv3
RC4_SHA_US	SSL_RSA_WITH_RC4_128_SHA	SSLv3
V 9.3.0 V 9.3.0 TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	TLSv1.3
V 9.3.0 V 9.3.0 TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	TLSv1.3
V 9.3.0 V 9.3.0 TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	TLSv1.3
TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSL_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1
TLS_RSA_WITH_AES_128_CBC_SHA	SSL_RSA_WITH_AES_128_CBC_SHA	TLSv1
TLS_RSA_WITH_AES_128_CBC_SHA256	SSL_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	SSL_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_CBC_SHA	SSL_RSA_WITH_AES_256_CBC_SHA	TLSv1
TLS_RSA_WITH_AES_256_CBC_SHA256	SSL_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	SSL_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_RSA_WITH_DES_CBC_SHA	SSL_RSA_WITH_DES_CBC_SHA	TLSv1
TLS_RSA_WITH_NULL_NULL	Není k dispozici	Není k dispozici
TLS_RSA_WITH_NULL_SHA256	SSL_RSA_WITH_NULL_SHA256	TLSv1.2
TLS_RSA_WITH_RC4_128_SHA256	SSL_RSA_WITH_RC4_128_SHA	TLSv1.2
TRIPLE_DES_SHA_US	SSL_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3

Navázání komunikace SSL/TLS v souboru MQIPT

Proces navázání komunikace SSL/TLS se vyskytne během počátečního požadavku na připojení mezi klientem a serverem SSL/TLS, když se provádí ověření a vyjednávání CipherSuites .

Všechny podporované sady SSL/TLS CipherSuites (viz “Podpora SSL/TLS v souboru MQIPT” na stránce 1010), s výjimkou anonymních sad CipherSuites, vyžadují ověření serveru a umožňují ověření klienta. Server lze nakonfigurovat tak, aby požadoval ověření klienta. Měli byste se vyhnout použití anonymních CipherSuites , protože neposkytují žádné záruky ohledně identity vzdáleného partnera. Je možné, aby útok typu man-in-the-middle zachytil anonymní spojení SSL/TLS bez vašeho vědomí. Anonymní CipherSuites používejte pouze v důvěryhodných interních sítích a pouze v případě, že jste připraveni přijmout riziko zachycení dat.

Ověření typu peer komunikace v SSL/TLS je založeno na šifrování pomocí veřejného klíče a digitálních certifikátech X.509v3 . Server, který by měl být ověřen v protokolu SSL/TLS, vyžaduje soukromý klíč a digitální certifikát (který obsahuje odpovídající veřejný klíč spolu s informacemi o identitě serveru), dobu platnosti certifikátu. Certifikáty jsou podepsány certifikační autoritou, certifikáty těchto autorit se nazývají certifikáty podepsaného. Certifikát následovaný jedním nebo více certifikáty podepsaného tvoří řetěz certifikátů. Řetěz certifikátů je charakterizován tím, že od prvního certifikátu (certifikátu serveru)

lze podpis každého certifikátu v řetězci ověřit pomocí veřejného klíče obsaženého v dalším certifikátu podepsaného.

Při vytváření zabezpečeného připojení, které vyžaduje ověření serveru, odešle server klientovi řetěz certifikátů, aby prokázal svou identitu. Klient SSL/TLS bude pokračovat v navázání připojení k serveru pouze v případě, že může ověřit server, například ověřit podpis certifikátu serveru. Aby bylo možné ověřit podpis, musí klient SSL/TLS důvěřovat serveru samotnému nebo alespoň jednomu z podepisujících subjektů v řetězu certifikátů poskytnutém serverem. Certifikáty důvěryhodných serverů a podepisujících subjektů musí být udržovány na straně klienta, aby bylo možné provést toto ověření.

Klient SSL/TLS zkontroluje řetěz certifikátů serveru, počínaje certifikátem serveru. Klient považuje podpis certifikátu lokality za platný za následujících okolností:

- Certifikát serveru je v úložišti důvěryhodného serveru nebo certifikátů podepsaného
- Certifikát podepsaného v řetězu lze ověřit na základě úložiště důvěryhodných certifikátů podepsaného.

V druhém případě klient SSL/TLS zkontroluje, zda je řetěz certifikátů skutečně správně podepsán, od důvěryhodného certifikátu podepsaného až po certifikát serveru. Každý certifikát zapojený do tohoto procesu je také přezkoumán na správnost formátu a data platnosti. Pokud se některá z těchto kontrol nezdaří, bude připojení k serveru odmítnuto. Po ověření certifikátu serveru klient použije veřejný klíč vložený do tohoto certifikátu v dalších krocích protokolu SSL/TLS. Připojení SSL/TLS lze navázat pouze v případě, že server skutečně má odpovídající soukromý klíč.

Ověření klienta se řídí stejným postupem: pokud server SSL/TLS vyžaduje ověření klienta, odešle klient na server řetěz certifikátů, aby prokázal svou identitu. Server ověřuje řetěz na základě úložiště důvěryhodného serveru a certifikátů podepsaného. Po ověření certifikátu klienta server použije veřejný klíč vložený do tohoto certifikátu v dalších krocích protokolu SSL/TLS. Připojení SSL/TLS lze navázat pouze v případě, že klient skutečně má odpovídající soukromý klíč.

Nedávné verze protokolů TLS poskytují vysokou úroveň zabezpečení komunikace (SSL a starší protokoly TLS jsou považovány za nezabezpečené). Protokol však funguje na základě informací poskytnutých aplikací. Pouze v případě, že je tato informační základna také bezpečně udržována, lze dosáhnout celkového cíle bezpečné komunikace. Pokud je například ohroženo úložiště důvěryhodných certifikátů serveru a podepsaného, můžete vytvořit zabezpečené připojení k velmi nezabezpečenému komunikačnímu partnerovi.

MQIPT implementace SSL/TLS

Protokoly SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 a TLS 1.3 jsou implementovány s tokeny PKCS (Public Key Cryptography Standards) #12 uloženými v souborech svazku klíčů (s typy souborů `.p12` nebo `.pfx`), které obsahují X509.V3 . Produkt MQIPT může také používat úložiště klíčů kryptografického hardwaru, která podporují standard PKCS#11 Cryptographic Token Interface. Produkt MQIPT používá balík IBM Java Secure Socket Extension (JSSE).

Produkt MQIPT může fungovat jako klient SSL/TLS nebo server SSL/TLS v závislosti na tom, který konec iniciuje připojení. Klient spustí připojení a server přijme požadavek na připojení. Je možné, aby přenosová cesta MQIPT fungovala jak jako klient, tak jako server. V tomto případě použití funkce režimu serveru proxy SSL/TLS obvykle poskytuje lepší výkon.

Je-li produkt MQIPT konfigurován pro režim serveru proxy SSL/TLS, předává data SSL/TLS pouze mezi dvěma koncovými body; neúčastní se komunikace výměnou potvrzení SSL/TLS a nevyžaduje žádné digitální certifikáty.

Ve verzích starších než IBM MQ 9.3.0produkt MQIPT nepředává data SNI (TLS Server Name Indication), která jsou přijata v příchozím připojení TLS prostřednictvím odchozího připojení TLS. To znamená, že certifikáty pro jednotlivé kanály určené pomocí atributu kanálu **CERTLABL** nelze použít pro připojení TLS mezi produktem MQIPT a správcem cílové fronty. Chcete-li použít certifikát pro každý kanál ve správci cílové fronty, musí pro připojení TLS, které prochází produktem MQIPT ve verzi dřívější než IBM MQ 9.3.0, směrování MQIPT používat režim serveru proxy SSL/TLS, který předá všechny řídicí toky TLS neporušené, včetně názvu SNI. V 9.3.0 Od IBM MQ 9.3.0, MQIPT lze nakonfigurovat tak, aby buď nastavil SNI pro připojení TLS na specifickou hodnotu, nebo aby prošel SNI přijatým na příchozím připojení

k přenosové cestě. Další informace o použití více certifikátů ve správci front s produktem MQIPTnaleznete v tématu “IBM MQ podpora více certifikátů s MQIPT” na stránce 1011.

Každá přenosová cesta MQIPT může být nezávisle konfigurována s vlastní sadou vlastností SSL/TLS. Další podrobnosti viz MQIPT vlastnosti směrování .

Šifrování hesla svazku klíčů v souboru MQIPT

Zašifrujte heslo použité k otevření souboru klíčového řetězce nebo k přístupu k šifrovacím hardwarem používaným produktem MQIPTpomocí příkazu **mqiptPW** . Zašifrované heslo může být použito jakoukoli z následujících vlastností: **SSLClientKeyRingPW**, **SSLClientCAKeyRingPW**, **SSLServerKeyRingPW**, **SSLServerCAKeyRingPW**a **SSLCommandPortKeyRingPW**. Toto téma popisuje správný způsob uložení hesla svazku klíčů pro použití produktem MQIPT.

Prostředek pro dočasné ukládání **mqiptkeyman** (iKeyman) není produktem MQIPTpodporován. Místo použití souboru pro dočasné ukládání musíte k uložení šifrovaného hesla použít příkaz **mqiptPW** .

Ve verzích starších než IBM MQ 9.1.5jsou hesla svazku klíčů pro použití produktem MQIPT uložena v souborech, na které odkazuje kterákoli z vlastností **SSL*KeyRingPW** .

V produktu IBM MQ 9.1.5zašifrujte hesla svazku klíčů pro použití produktem MQIPT pomocí příkazu **mqiptPW** a nastavte hodnotu vlastností **SSL*KeyRingPW** na zašifrované heslo. Produkt MQIPT je schopen rozlišovat mezi zašifrovanými hesly a názvy souborů v hodnotách vlastností kvůli kompatibilitě s konfiguracemi vytvořenými před produktem IBM MQ 9.1.5.

Deprecated Metoda šifrování hesel úložiště klíčů, která je k dispozici ve starších verzích systému MQIPT než IBM MQ 9.1.5 , je zamítnuta, ale lze ji i nadále používat. Chcete-li zlepšit ochranu hesel klíčového řetězce, znovu zašifrujte všechna hesla klíčového řetězce, která byla dříve zašifrována, pomocí nejnovější metody ochrany.

Chcete-li šifrovat heslo svazku klíčů pro použití produktem MQIPT, postupujte podle pokynů v části “Šifrování uložených hesel v adresáři MQIPT” na stránce 1046.

Musíte použít heslo `mqiptSample` k otevření jednoho z ukázkových souborů klíčového řetězce dodaných v podadresáři `samples/ssl` instalačního adresáře MQIPT .

Výběr certifikátů ze souboru svazku klíčů v adresáři MQIPT

Je možné, aby byl ve stejném souboru klíčového řetězce nebo šifrovacím hardwarovém tokenu uložen více než jeden osobní certifikát. Vlastnosti **SSLClientSite*** lze použít na straně klienta k výběru certifikátu, který má být odeslán k ověření na server, a vlastnosti **SSLServerSite*** lze použít na straně serveru k výběru certifikátu, který má být odeslán klientovi k ověření.

Pomocí těchto vlastností lze vybrat certifikát na základě jeho rozlišujícího názvu (DN). Případně lze popisek certifikátu použít k výběru certifikátu pomocí vlastností **SSLServerSiteLabel** a **SSLClientSiteLabel** .

Chcete-li vybrat certifikát serveru používaný příkazovým portem TLS, použijte vlastnost **SSLCommandPortSiteLabel** k určení názvu popisku certifikátu.

Nastavení důvěryhodnosti v souboru MQIPT

Svazek klíčů obsahuje osobní certifikát, který zahrnuje certifikát podepsaného nebo řetěz certifikátů podepsaného.

Existují dva typy kroužků klíčů používaných produktem MQIPT:

Svazek klíčů certifikační autority (CA)
Tento svazek klíčů obsahuje důvěryhodné certifikáty CA, které se používají k ověření certifikátů náležejících vzdálenému serveru typu peer. Tyto certifikáty CA pomáhají určit, zda je vzdálený peer důvěryhodný. Produkt MQIPT podporuje soubory svazku klíčů ve formátu PKCS #12 i úložiště šifrovacích hardwarových klíčů, která podporují rozhraní PKCS #11 , pro ukládání certifikátů CA. Soubory svazku klíčů CA MQIPT jsou identifikovány pomocí vlastností směrování **SSLClientCAKeyRing** a **SSLServerCAKeyRing** . Použití šifrovacího hardwaru pro přístup

k certifikátům CA je povoleno nastavením vlastností **SSLClientCAKeyRingUseCryptoHardware** a **SSLServerCAKeyRingUseCryptoHardware** .

Svazek klíčů CA na straně klienta SSL/TLS by měl obsahovat seznam důvěryhodných certifikátů CA, které budou použity k ověření certifikátu odeslaného ze serveru. Pokud je pro ověření klienta konfigurována trasa serveru SSL, svazek klíčů CA na straně serveru SSL/TLS by měl obsahovat seznam důvěryhodných certifikátů CA, které budou použity k ověření certifikátu odeslaného z klienta.

Svazek klíčů osobního certifikátu
Tento svazek klíčů obsahuje osobní certifikáty, které produkt MQIPT používá k identifikaci sebe sama na vzdáleném serveru typu peer. Při generování certifikátu podepsaného držitelem nebo vyžádání certifikátu podepsaného CA byste tak měli učinit pomocí svazku klíčů osobního certifikátu. Produkt MQIPT podporuje soubory svazku klíčů ve formátu PKCS #12 i úložiště klíčů kryptografického hardwaru, která podporují rozhraní PKCS #11 , pro ukládání osobních certifikátů. V produktu MQIPTjsou soubory svazku klíčů osobního certifikátu identifikovány pomocí vlastností směrování **SSLClientKeyRing** a **SSLServerKeyRing** . Použití šifrovacího hardwaru pro přístup k osobním certifikátům je povoleno nastavením vlastností **SSLClientKeyRingUseCryptoHardware** a **SSLServerKeyRingUseCryptoHardware** .

Svazek klíčů na straně serveru SSL/TLS by měl obsahovat osobní certifikát serveru MQIPT . Pokud je vyžadováno ověření klienta na trase klienta SSL, svazek klíčů na straně klienta SSL/TLS by měl obsahovat osobní certifikát klienta.

Pokud potřebujete ověření klienta, musíte na straně serveru povolit vlastnost **SSLServerAskClientAuth** . Svazek klíčů na straně klienta by měl obsahovat osobní certifikát klienta. Svazek klíčů MQIPT na straně serveru, identifikovaný vlastností **SSLServerCAKeyRing** , by měl obsahovat seznam důvěryhodných certifikátů CA, které budou použity k ověření klienta.

Pokud nekonfigurujete svazek klíčů CA pro trasu, produkt MQIPT bude místo toho hledat certifikáty CA v svazku klíčů osobního certifikátu, pokud je konfigurován. Není-li například pro parametr **SSLServerCAKeyRing**nastavena žádná hodnota, produkt MQIPT vyhledá certifikáty CA v svazku klíčů identifikovaném pomocí **SSLServerKeyRing**.

Jako alternativu k použití certifikátů podepsaných důvěryhodnou CA můžete použít certifikáty podepsané sebou samým. Příklad certifikátu podepsaného sebou samým najdete v ukázkovém souboru svazku klíčů `sslSample.pfx` , který je poskytován s produktem MQIPT v podadresáři `samples/ssl` . Chcete-li otevřít ukázkové soubory svazku klíčů PKCS#12 , musíte použít heslo `mqiptSample`.

Certifikáty podepsané svým držitelem mohou být užitečné v testovacích scénářích, kde musíte zajistit konektivitu SSL/TLS bez placení certifikační autority za certifikát. V produkčních prostředích byste však neměli používat certifikáty podepsané svým držitelem. Chcete-li vytvořit certifikát podepsaný certifikační autoritou, přečtěte si téma Vytvoření souboru klíčového řetězce.

Ke správě digitálních certifikátů a úložišť klíčů můžete použít obslužný program s názvem **mqiptkeyman**, který je součástí produktu MQIPT. Pokyny k instalaci a další informace naleznete v části “mqiptKeyman a mqiptKeycmd v MQIPT” na stránce 1024 .

Chcete-li zabránit neoprávněnému přístupu k souborům svazku klíčů a souborům hesel, musíte je chránit pomocí funkcí zabezpečení operačního systému.

Testování SSL/TLS v adresáři MQIPT

Příklady, které vám pomohou testovat připojení SSL/TLS.

Popis různých scénářů viz Začínáme s produktem IBM MQ Internet Pass-Thru . Viz zejména následující úlohy:

- Ověřování serveru SSL/TLS
- Ověřování klienta SSL/TLS
- Spuštění MQIPT v režimu serveru proxy SSL/TLS
- Spuštění MQIPT v režimu serveru proxy SSL/TLS se správcem zabezpečení

Chcete-li otestovat, zda vaše konfigurace SSL/TLS funguje správně, můžete použít certifikáty podepsané svým držitelem. Certifikáty podepsané svým držitelem jsou užitečné v testovacích scénářích, takže můžete zajistit konektivitu SSL/TLS bez placení certifikační autority (CA) za certifikát. Podrobnosti viz Vytvoření testovacích certifikátů .

Příklad certifikátu podepsaného sebou samým najdete v ukázkovém souboru svazku klíčů `sslSample.pfx` , který je poskytován s produktem MQIPT v podadresáři `samples/ssl` . Chcete-li otevřít ukázkové soubory svazku klíčů PKCS #12 , musíte použít heslo `mqiptSample`. Vzorový certifikát je poskytován pro vaše pohodlí během testování. Soukromé klíče ukázkového certifikátu jsou však známy všem uživatelům produktu MQIPT . To znamená, že je nejistý a měl by být používán pouze v testovacím prostředí.

V produkčních prostředích byste neměli používat žádné certifikáty podepsané sebou samým, bez ohledu na to, zda se jedná o ukázkové certifikáty. Namísto toho získejte certifikát podepsaný CA od důvěryhodné CA. Chcete-li vytvořit certifikát podepsaný certifikační autoritou, přečtěte si téma Vytvoření souboru klíčového řetězce.

Při vytváření nebo vyžádání certifikátu byste měli zvážit, který typ klíče, velikost klíče a algoritmus digitálního podpisu jsou vhodné pro vaše potřeby zabezpečení. Další informace viz “Aspekty digitálních certifikátů pro produkt MQIPT” na stránce 1026.

Certifikáty a technologie správy certifikátů jsou k dispozici od řady dodavatelů třetích stran.

Chybové zprávy SSL/TLS v souboru MQIPT

Selhání navázání komunikace se protokolují do protokolu připojení MQIPT ve formě výjimek JSSE.

Další informace viz téma “Protokoly připojení v adresáři MQIPT” na stránce 1049. Následující tabulka popisuje různé výjimky, pravděpodobnou příčinu a odpovídající akci pro vyřešení selhání.

Výjimky certifikátu se obvykle vztahují k certifikátům na vzdáleném konci připojení.

Pokud se chyba týká certifikátu klienta IBM MQ nebo správce front, termín *soubor klíčového řetězce* zahrnuje úložiště klíčů IBM MQ vzdáleného partnera.

V produktu MQIPTjsou certifikáty CA uloženy v souboru svazku klíčů CA, který je identifikován vlastnostmi trasy **SSLClientCAKeyRing** a **SSLServerCAKeyRing** . Pokud nejsou nastaveny vlastnosti trasy svazku klíčů CA, bude místo toho vyhledán odpovídající soubor svazku osobních klíčů (odkazovaný vlastností **SSLClientKeyRing** nebo **SSLServerKeyRing**) pro certifikáty CA.

Výjimka	Příčina	Akce
CertificateException	Certifikát není důvěryhodný, protože je podepsán certifikační autoritou, která není v svazku klíčů certifikační autority.	Zkontrolujte, zda jsou v souboru svazku klíčů CA obsaženy všechny potřebné certifikáty CA. Pomocí nástroje IBM Správa klíčů dodávaného s produktem MQIPT přidejte všechny chybějící certifikáty CA, přičemž je třeba dbát na to, abyste získali kopii každého certifikátu CA z důvěryhodného zdroje.
Výjimka CertificateExpired	1. Certifikátu vypršela platnost: datum **notAfter** uplynulo. 2. Systémové hodiny jsou nastaveny nesprávně.	1. Získejte nový certifikát a vložte jej do souboru svazku klíčů. Pokud certifikát patří certifikační autoritě, umístěte nový certifikát do souboru svazku klíčů certifikační autority. 2. Zkontrolujte, zda jsou systémové hodiny UTC nastaveny na správný čas.

Výjimka	Příčina	Akce
CertificateNotYetValidVýjimka	1. Certifikát se používá předčasně: jeho datum **notBefore** ještě nebylo doručeno. 2. Systémové hodiny jsou nastaveny nesprávně.	1. Zkontrolujte, zda byl certifikát správně vygenerován a podepsán. Pokud vaše organizace provozuje vlastní certifikační autoritu, může být systémový čas UTC pro certifikační autoritu nesprávný. 2. Zkontrolujte, zda jsou systémové hodiny UTC nastaveny na správný čas.
Výjimka CertificateParsing	1. Certifikát obsahuje neplatná data DER. 2. Certifikát používá nepodporované funkce DER.	Ujistěte se, že byl certifikát správně vygenerován a lze jej zobrazit v IBM nástroji pro správu klíčů dodaném s produktem MQIPT. Zvažte získání nového certifikátu s menším počtem rozšíření certifikátu.
Výjimka CertificateRevoked	Kontrola odvolání certifikátu je povolena a bylo zjištěno, že certifikát byl odvolán.	Daný certifikát by neměl být důvěryhodný. Získejte náhradní certifikát a ujistěte se, že nový certifikát a jeho soukromý klíč jsou přítomny v souboru svazku klíčů.
CertPathBuilderException	Řetěz certifikátů nebyl podepsán uznávanou certifikační autoritou.	1. Používáte-li certifikáty podepsané certifikační autoritou, zkontrolujte, zda jsou v souboru svazku klíčů certifikační autority přítomny všechny kořenové a přechodné certifikáty certifikační autority. 2. Používáte-li certifikáty podepsané držitelem, ujistěte se, že jste extrahovali kopii veřejné části vzdáleného certifikátu a přidali ji do souboru svazku klíčů CA. Vyvarujte se použití certifikátů podepsaných sebou samým v produkčních prostředích.

Výjimka	Příčina	Akce
Výjimka CertStore Výjimka KeyStore	Při čtení certifikátu ze svazku klíčů došlo k chybě z jednoho z následujících důvodů: 1. Soubor klíčového řetězce je poškozen. 2. Chybí soubor klíčového řetězce. 3. Uložené heslo neodpovídá heslu souboru klíčového řetězce. 4. Je-li přenosová cesta konfigurována pro použití šifrovacího hardwaru, produkt MQIPT se nemůže připojit k šifrovanému hardwaru.	1. Ujistěte se, že soubor svazku klíčů lze číst a že všechny certifikáty lze zobrazit pomocí nástroje Správa klíčů IBM . 2. Zkontrolujte, zda všechny vlastnosti přenosové cesty klíčového řetězce odkazují na správný název souboru. 3. Zkontrolujte, zda je heslo k uloženému souboru svazku klíčů správné. Pomocí nástroje **mqiptPW** uložte správné heslo. 4. Pokud je přenosová cesta konfigurována pro použití šifrovacího hardwaru, zkontrolujte následující: • Soubor vlastností zabezpečení Java uvádí, že je nainstalován poskytovatel zabezpečení IBMPKCS11Impl . • Soubor vlastností zabezpečení Java obsahuje úplný název konfiguračního souboru, který se používá k inicializaci poskytovatele zabezpečení IBMPKCS11Impl . • Konfigurační soubor použitý k inicializaci poskytovatele zabezpečení IBMPKCS11Impl je platný.
SSLException: Žádný dostupný certifikát nebo klíč neodpovídá šifrovaným sadám SSL, které jsou povoleny.	Musíte mít osobní certifikát se správným typem klíče pro CipherSuites , které používáte. Například CipherSuites , jejichž názvy začínají na SSL_ECDH_ECDSA_ , vyžadují certifikát s veřejným klíčem Elliptic Curve. Nejčastěji používané CipherSuites vyžadují certifikát s veřejným klíčem RSA.	Otevřete soubor svazku klíčů pomocí nástroje Správa klíčů IBM . V pohledu Osobní certifikáty postupně vyberte jednotlivé certifikáty a zobrazte je. Klepněte na volbu **Zobrazit podrobnosti** a přejděte do sekce Veřejný klíč předmětu, abyste viděli typ veřejného klíče. Poté zkontrolujte vlastnosti směrování MQIPT **SSLClientCipherSuites** a **SSLServerCipherSuites** a ujistěte se, že jsou povoleny příslušné CipherSuites .

Výjimka	Příčina	Akce
SSLException: Nejsou společné žádné šifrovací sady SSLHandshakeException: Nejsou žádné společné šifrovací sady.	Navázání komunikace se nepodařilo schválit sadu CipherSuite , protože se mezi sadami povolených CipherSuites na obou koncích připojení nepřekrývají. Zejména odchozí připojení IBM MQ povoluje pouze jedinou šifru, takže přenosové cesty SSLServer MQIPT pravděpodobně tuto chybu zaznamenají. K této chybě může dojít také v případě, že jsou splněny všechny tři následující podmínky: • na trase není uvedena žádná sada CipherSuite • v svazku klíčů konfigurovaném pro trasu nebyl nalezen žádný vhodný certifikát lokality • anonymní CipherSuites jsou zakázány	Zkontrolujte seznam povolených CipherSuites ve vlastnostech směrování MQIPT **SSLClientCipherSuites** a **SSLServerCipherSuites** . Zvažte povolení dalších CipherSuites. V poskytnuté tabulce určete správné sady CipherSuites , které mají být povoleny pro jednotlivé hodnoty IBM MQ kanálu CipherSpec . Není-li na trase zadána žádná sada CipherSuite , zkontrolujte, zda vlastnosti trasy klíčového řetězce odkazují na správný soubor klíčového řetězce a zda svazek klíčů obsahuje osobní certifikát, který může produkt MQIPT používat. Je-li přenosová cesta konfigurována pro použití šifrovacího hardwaru, zkontrolujte, zda atribut **tokenlabel** v konfiguračním souboru, který se používá k inicializaci poskytovatele zabezpečení IBMPKCS11Impl , určuje správný popisek tokenu šifrovacího zařízení.

mqiptKeyman a mqiptKeycmd v MQIPT

mqiptKeyman (iKeyman) je aplikace pro správu certifikátů a klíčů, která je uživatelům produktu IBM MQ již známa. Příkazy **mqiptKeyman** a **mqiptKeycmd** lze použít ke správě symetrických a asymetrických klíčů, digitálních certifikátů a žádostí o certifikáty v souborech klíčového řetězce používaných produktem IBM MQ Internet Pass-Thru. Tyto soubory lze také použít ke správě samotných souborů klíčového řetězce.

Příkazy **mqiptKeyman** a **mqiptKeycmd** používají výraz *databáze klíčů* k odkazování na soubor klíčového řetězce; tyto výrazy jsou synonymní.

iKeyman lze spustit ve dvou režimech, grafickém uživatelském rozhraní (GUI) a rozhraní příkazového řádku (CLI). Použijte příkaz **mqiptKeyman** ke spuštění grafického rozhraní a příkaz **mqiptKeycmd** ke spuštění rozhraní příkazového řádku.

Ekvivalentní příkazy pro správu certifikátů v produktu IBM MQ jsou **strmqikm** pro spuštění grafického rozhraní a **runmqckm** pro spuštění rozhraní příkazového řádku. Příkazy IBM MQ jsou popsány v části Použití **runmqckm**, **runmqakm**a **strmqikm** ke správě digitálních certifikátů.

Poznámka: Deprecated V 9.3.4 Nástroje **mqiptKeycmd** a **mqiptKeyman** jsou zamítnuty produktem IBM MQ 9.3.4. Další informace naleznete v tématu Použití **runmqckm**, **runmqakm**a **strmqikm** ke správě digitálních certifikátů.

Požadovaný formát souboru klíčového řetězce pro MQIPT

Při vytváření souborů klíčového řetězce pro použití v produktu MQIPTmusíte použít formát souboru PKCS #12 :

- V uživatelském rozhraní vyberte volbu PKCS#12 v poli **Typ databáze klíčů** při vytváření souboru klíčového řetězce.

- V rozhraní příkazového řádku uveďte parametr `-type pkcs12` v příkazu `mqiptKeycmd -keydb -create` .

Produkt MQIPT může také přistupovat k certifikátům uloženým v šifrovacím hardwaru, který podporuje rozhraní PKCS #11 . Rozhraní lze také použít ke správě certifikátů na hardwaru PKCS #11 . Další informace viz téma “Použití šifrovacího hardwaru PKCS #11 v produktu MQIPT” na stránce 1034.

Šifrování hesla svazku klíčů pro MQIPT

Po vytvoření souboru svazku klíčů musíte zašifrovat heslo svazku klíčů ve formátu, který může produkt MQIPT použít pro přístup k souboru. Informace o tomto tématu viz “Šifrování hesla svazku klíčů v souboru MQIPT” na stránce 1019 .

Všimněte si, že prostředek pro soubor pro dočasné ukládání není produktem MQIPTpodporován. K zašifrování hesla svazku klíčů namísto použití souboru pro dočasné ukládání musíte použít příkaz **mqiptPW** .

Příklady příkazového řádku

Rozhraní příkazového řádku používá stejnou syntaxi jako příkaz IBM MQ **runmqckm** . Připojte požadované parametry k souboru **mqiptKeycmd**, jak je znázorněno v následujících příkladech:

- Chcete-li vytvořit soubor PKCS#12 , postupujte takto:

```
mqiptKeycmd -keydb -create -db key.p12 -pw password -type pkcs12
```

- Chcete-li vytvořit osobní certifikát podepsaný svým držitelem pro účely testování, postupujte takto:

```
mqiptKeycmd -cert -create -db key.p12 -pw password -type pkcs12
-label mqipt -dn "CN=Test Certificate,OU=Sales,O=Example,C=US"
-sig_alg SHA256WithRSA -size 2048
```

  Příkaz vytvoří digitální certifikát s 2048bitovým veřejným klíčem RSA a digitálním podpisem, který používá RSA s hašovacím algoritmem SHA-256 . Při vytváření certifikátu dávejte pozor na výběr algoritmu šifrování veřejného klíče, velikosti klíče a algoritmu digitálního podpisu, který odpovídá potřebám zabezpečení vaší organizace. Další informace viz “Aspekty digitálních certifikátů pro produkt MQIPT” na stránce 1026.

  Tento příklad používá certifikát podepsaný svým držitelem, který je vhodný pro testovací účely. V produkčním prostředí byste však měli místo toho použít podepsaný certifikát certifikační autority.

  Všimněte si, že produkt MQIPT v2.0 a starší verze nepodporují digitální podpisy SHA-2 , takže tento certifikát není vhodný pro vytvoření připojení zabezpečeného soketu k předchozím vydáním produktu MQIPT ; starší podpisový algoritmus, jako například SHA1WithRSA, by byl požadován.

- Chcete-li vytvořit žádost o certifikát pro certifikát podepsaný certifikační autoritou pro produkční účely, postupujte takto:

```
mqiptKeycmd -certreq -create -db key.p12 -pw password -type pkcs12 -file cert.req
-label mqipt -dn "CN=Test Certificate,OU=Sales,O=Example,C=US"
-sig_alg SHA256WithRSA -size 2048
```

  Příkaz vytvoří požadavek na digitální certifikát s 2048bitovým veřejným klíčem RSA a digitálním podpisem, který používá RSA s hašovacím algoritmem SHA-256 . Při vytváření certifikátu dávejte pozor na výběr algoritmu šifrování veřejného klíče, velikosti klíče a algoritmu digitálního podpisu, který odpovídá potřebám zabezpečení vaší organizace. Další informace viz “Aspekty digitálních certifikátů pro produkt MQIPT” na stránce 1026.

- Chcete-li přijmout soubor osobního certifikátu podepsaného certifikační autoritou `cert.crt` do souboru svazku klíčů, postupujte takto:

```
mqiptKeycmd -cert -receive -db key.p12 -pw password -type pkcs12 -file cert.crt
```

  Musíte se ujistit, že certifikát CA, který podepsal osobní certifikát, je přítomen v souboru svazku klíčů CA, například:

```
mqiptKeycmd -cert -add -db key.p12 -pw password -type pkcs12 -file ca.crt -label rootCA
```

Aspekty digitálních certifikátů pro produkt MQIPT

Zvažte například velikost klíče certifikátu, výběr vhodného algoritmu digitálního podpisu certifikátu a digitálního certifikátu a kompatibilitu certifikátu CipherSuite compatibilityDigital a CipherSuite .

Aspekty velikosti klíče certifikátu pro MQIPT

Velikost veřejného klíče závisí na zásadách zabezpečení vaší organizace a závisí na použitém šifrovacím algoritmu. Obecně platí, že větší velikosti klíčů jsou bezpečnější. V následující tabulce jsou uvedeny minimální velikosti klíčů, které byste měli použít:

algoritmus	**Minimální velikost klíče (bity)**
Eliptická křivka	256
RSA	2048

Při vytváření certifikátu nebo žádosti o certifikát zadejte velikost klíče certifikátu.

- Při použití příkazu rozhraní příkazového řádku **mqiptKeycmd** parametr **-size** uvádí velikost klíče.
- Při použití grafického rozhraní **mqiptKeyman** uvádí velikost klíče pole **Velikost klíče** v okně Vytvoření certifikátu.

Výběr vhodného algoritmu digitálního podpisu certifikátu

Chcete-li zabránit padělání digitálních certifikátů, je důležité použít silný algoritmus digitálního podpisu. Když vytváříte nebo požadujete certifikát, dávejte pozor na výběr správného algoritmu.

Měli byste se vyvarovat použití starých algoritmů digitálního podpisu založených na MD5 nebo SHA-1 , protože tyto algoritmy již nejsou dostatečně bezpečné pro moderní použití. Je-li to možné, použijte jeden z novějších algoritmů digitálního podpisu založených na SHA-2 , například SHA-256 s RSA (SHA256WithRSA).

Avšak verze produktu MQIPT starší než verze 2.1 nepodporují digitální podpisy SHA-2 , takže pro interoperabilitu s předchozími verzemi produktu MQIPT použijte algoritmus digitálního podpisu SHA1WithRSA . Měli byste však naplánovat upgrade starších verzí produktu MQIPT a fázovat používání digitálních podpisů MD5 a SHA-1 .

- Při použití příkazu rozhraní příkazového řádku **mqiptKeycmd** parametr **-sig_alg** uvádí algoritmus digitálního podpisu.
- Při použití grafického rozhraní **mqiptKeyman** uvádí pole **Algoritmus podpisu** v okně Vytvoření certifikátu algoritmus digitálního podpisu.

Digitální certifikát a kompatibilita CipherSuite v produktu MQIPT

Ne všechny CipherSuites lze použít se všemi digitálními certifikáty. Existují různé typy sady CipherSuiteseskupené podle jejich předpony názvu CipherSuite . Každý typ CipherSuite ukládá různá omezení typu digitálního certifikátu, který lze použít. Tato omezení platí pro všechna připojení SSL/TLS v systému MQIPT , ale jsou zvláště relevantní pro uživatele šifrování Elliptic Curve. Při provádění komunikace výměnou potvrzení zabezpečeného soketu produkt MQIPT automaticky vybere osobní

certifikát, který identifikuje sám sebe a který je vhodný pro vyjednanou CipherSuite. Ve většině případů produkt MQIPT automaticky spolupracuje se vzdáleným peerem. V některých scénářích však může být nutné použít specifickou sadu MQIPT CipherSuite pro spolupráci se vzdáleným systémem IBM MQ . Aplikace **mqiptKeyman** dodávaná s produktem MQIPT je schopna vytvářet certifikáty a žádosti o certifikáty pouze s veřejnými klíči DSA a RSA. Kromě toho může obslužný program IBM MQ **runmqakm** vytvářet certifikáty a požadavky na certifikáty pomocí veřejných klíčů Elliptic Curve. Informace o vytváření dalších typů certifikátů vám poskytne certifikační autorita.

Typ digitálního certifikátu, který se má použít, závisí na typu používané sady CipherSuite :

- CipherSuites s názvy začínajícími znaky SSL_ECDH_ECDSA_ a SSL_ECDHE_ECDSA_ vyžadují digitální certifikát s veřejným klíčem Elliptic Curve.
- CipherSuites s názvy, které obsahují *anon* , jsou anonymní. K identifikaci vzdáleného partnera nevyžadují digitální certifikát. Takové CipherSuites se mohou vyvarovat režijních nákladů správy životního cyklu certifikátů v sítích, kde se používají alternativní prostředky ověření, ale obecně se vyvarují jejich použití kvůli nedostatku ověření.
- Jiné CipherSuites vyžadují digitální certifikát s veřejným klíčem RSA.

Poznámka: Nástroje **mqiptKeyman** a **mqiptKeycmd** nemohou vytvářet certifikáty nebo požadavky na certifikáty s veřejným klíčem Elliptic Curve. K tomuto účelu můžete použít příkaz **runmqakm** poskytnutý s produktem IBM MQ . Příkaz **runmqakm** je popsán v části Použití **runmqckm**, **runmqakm**a **strmqikm** ke správě digitálních certifikátů.

Uživatelská procedura certifikátu v adresáři MQIPT

Účelem uživatelské procedury certifikátu je ověřit certifikát typu peer SSL/TLS, který je přijat produktem MQIPT.

Přenosovou cestu MQIPT můžete nakonfigurovat tak, aby se chovala jako klient SSL/TLS, když vytváří nové připojení, a aby se chovala jako server SSL/TLS, když obdrží požadavek na připojení. Během procesu navázání komunikace SSL/TLS klient SSL/TLS obdrží od serveru certifikát typu peer a certifikát lze použít k ověření serveru. Server SSL/TLS může také obdržet certifikát typu peer od klienta a tento certifikát lze použít k ověření klienta.

Uživatelská procedura certifikátu je volána, když produkt MQIPT obdrží certifikát typu peer, který vám umožní provést další ověření. Všechny výjimky zachycené uživatelskou procedurou jsou zachyceny produktem MQIPT a požadavek na připojení byl ukončen. Proto je dobrým zvykem, aby uživatelská procedura zachytila všechny výjimky a předala zpět odpovídající návratový kód do MQIPT.

Další informace naleznete v tématu Použití uživatelské procedury certifikátu k ověření serveru SSL/TLS.

Poznámka: Produkt MQIPT je spuštěn v jednom produktu Java Virtual Machine , takže uživatelská procedura certifikátu může ohrozit normální provoz produktu MQIPT jedním z těchto způsobů:

- Ovlivnit systémové prostředky
- Generovat kritická místa
- Snížit výkon

Před implementací certifikátu v produkčním prostředí byste měli důkladně otestovat účinky ukončení certifikátu.

Třída com.ibm.mq.ipt.exit.CertificateExit v souboru MQIPT

Třída com.ibm.mq.ipt.exit.CertificateExit je abstraktní třída, která musí být implementována třídou, která je definována s vlastností SSLExitName .

Třída obsahuje výchozí implementace pro spuštění uživatelské procedury a některé veřejné metody, které můžete volitelně přepsat podle svých požadavků. Úplný seznam podporovaných metod je následující:

metody

public int init (IPTTrace) (veřejná vnitřní inicializace)

Metoda init je volána produktem MQIPT , když je uživatelská procedura načtena produktem MQIPT , a může být implementována k provedení jakékoli inicializace uživatelské procedury; například načtení dat, která se používají během procesu ověření. Výchozí implementace neprovádí nic.

public int refresh (IPTTrace) (veřejná obnova int)

Metoda aktualizace je implementována k provedení aktualizace libovolných dat; například k opětovnému načtení všech dat pro disk, která se používají během procesu ověření. Tato metoda se volá, když administrátor MQIPT zadá příkaz refresh. Výchozí implementace neprovádí nic.

public void close (IPTTrace) (veřejné anulování)

Metoda zavření je implementována k provedení úklidu, když se trasa zastaví, nebo když se produkt MQIPT zavírá. Výchozí implementace neprovádí nic.

public CertificateExit-ověření odezvy (IPTTrace)

Metoda ověření je volána k provedení ověření rovnocenného certifikátu. Návratový objekt lze použít k předání informací zpět do produktu MQIPT; například návratový kód a nějaký text, který lze přidat do protokolu připojení. Výchozí implementace vrátí odezvu CertificateExits CertificateExitResponse.OK.

Podporované metody pro získání vlastností:

public int getListenerPort () (
načte port modulu listener trasy-jak je definováno vlastností ListenerPort

public String getDestination()
načte cílovou adresu-jak je definováno vlastností Destination

public int getDestinationPort ()
načte adresu cílového portu modulu listener-jak je definováno vlastností DestinationPort

veřejný řetězec getClientIPAddress ()
načte adresu IP klienta, který vytváří požadavek na připojení

public int getClientPortAddress()
načte adresu portu používanou klientem, který zadává požadavek na připojení

public boolean isSSLClient()
k určení, zda je uživatelská procedura volána jako klient SSL/TLS nebo server SSL/TLS. Pokud se vrátí hodnota true, uživatelská procedura se nachází na straně klienta připojení a ověřuje se certifikát získaný ze serveru. Pokud tato volba vrátí hodnotu false, uživatelská procedura je na straně serveru připojení a ověřuje certifikát odeslaný klientem. Je platné, aby přenosová cesta fungovala jak jako server SSL/TLS, tak jako klient SSL/TLS, který dešifruje a znovu šifruje provoz. V této situaci, i když existuje jediná třída ukončení, budou některé instance třídy volány jako klienti a některé jako servery. Pomocí příkazu isSSLClient můžete určit situaci pro danou instanci.

public int getConnThreadID()
Používá se k načtení ID pracovního podprocesu, který zpracovává požadavek na připojení, což může být užitečné pro ladění.

veřejný řetězec getChannelname ()
načte název kanálu IBM MQ , který se používá v požadavku na připojení. Tato volba je k dispozici pouze v případě, že příchozí požadavek nepoužívá protokol SSL/TLS a produkt MQIPT vystupuje jako klient SSL/TLS.

public String getQMName()
načte název správce front IBM MQ použitého v požadavku na připojení. Tato volba je k dispozici pouze v případě, že požadavek klienta nepoužívá protokol SSL/TLS a produkt MQIPT vystupuje jako klient SSL/TLS.

public boolean getTimedout()
použitý uživatelskou procedurou k určení, zda vypršel časový limit.

public IPTCertificate getCertificate()
načte certifikát SSL/TLS, který je třeba ověřit.

public String getExitData ()
načte data uživatelské procedury, jak je definováno vlastností SSLExitData .

veřejný řetězec getExitName ()
načte název uživatelské procedury, jak je definováno vlastností SSLExitName .

Třída com.ibm.mq.ipt.exit.CertificateExitResponse v souboru MQIPT

Tato třída se používá k předání informací zpět do produktu MQIPT po ověření certifikátu.

Konstruktory

public CertificateExitResponse (*int rc*, řetězcová zpráva)

Tento konstruktor lze použít k předání návratového kódu a textu zprávy. Možné kódy příčiny jsou

- ExitRc.OK
- ExitRc.VALIDATE_ERROR
- ExitRc.OVĚŘIT_ODMÍTNUTO

public CertificateExitResponse (*int rc*)

Tento konstruktor lze použít k předání návratového kódu bez textu zprávy. Možné kódy příčiny jsou

- ExitRc.OK
- ExitRc.VALIDATE_ERROR
- ExitRc.OVĚŘIT_ODMÍTNUTO

public CertificateExitresponse () (odpověď)

Tento konstruktor lze použít k předání návratového kódu ExitRc.OK, bez textu zprávy.

metody

public String getVersion()

Tato metoda vrací verzi této třídy.

veřejný řetězec toString

Tato metoda vrátí řetězcovou reprezentaci odezvy, například " Kód příčiny: 4, Zpráva: Nezdařená kontrola CRL.

Třída com.ibm.mq.ipt.exit.IPTCertificate v souboru MQIPT

Tato třída obsahuje certifikát SSL/TLS, který má být ověřen.

metody

veřejný int getVersion()

Tato metoda vrací verzi této třídy.

veřejný bajt [] getDerEncoding ()

Tato metoda vrátí kódování ASN.1/DER certifikátu X.509 nebo hodnotu NULL, pokud dojde k chybě.

veřejný bajt [] getPemEncoding ()

Tato metoda vrací kódování PEM (BASE64) certifikátu X.509 nebo hodnotu NULL, pokud dojde k chybě.

veřejný řetězec getLabel()

Tato metoda vrátí popisek certifikátu nebo hodnotu NULL, pokud dojde k chybě.

veřejný řetězec getName()

Tato metoda vrátí rozlišující název certifikátu, nebo hodnotu NULL, pokud není k dispozici. Příklad:

```
CN=Test Queue Manager,OU=Sales,O=Example,L=London,C=GB
```

public String getIssuerName ()

Tato metoda vrací rozlišující název vydavatele certifikátu nebo hodnotu NULL, pokud není k dispozici. Příklad:

```
CN=Certificate Authority,OU=Security,O=Example,L=New York,C=US
```

public IPTCertificate getSigner()

Tato metoda vrátí certifikát podepsaného nebo hodnotu NULL, není-li k dispozici. Pro certifikát podepsaný svým držitelem vrátí odkaz na sebe sama.

public String toString()

Tato metoda vrací řetězcovou reprezentaci certifikátu.

Třída com.ibm.mq.ipt.exit.IPTTrace v souboru MQIPT

Funkce trasování MQIPT poskytují vstupní a výstupní volání, která lze použít při vstupu a výstupu z metody. K dispozici jsou také různá datová volání pro trasování užitečných informací.

metody

public void entry (String *fid*) (veřejná neobsazená položka)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody.

Tato metoda zapíše položku do výstupního souboru trasování s odpovídající úrovní odsazení, aby zaznamenala bod, ve kterém tok řízení vstupuje do metody. Toto volání je volitelné, ale pokud je použito, odpovídající volání "exit (String)" musí být také použito v rámci stejné metody.

public void exit (String *fid*)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody.

Tato metoda zapíše uživatelskou proceduru do výstupního souboru trasování s odpovídající úrovní odsazení, aby zaznamenala bod, ve kterém tok řízení opouští metodu. Tato metoda se používá pouze v případě, že bylo dříve použito volání "entry (String)" v rámci stejné metody.

public void exit (String *fid*, int *rc*)

Kde *fid* se používá k identifikaci, kde bylo volání provedeno, například název třídy a metody, a *rc* je číselný návratový kód z metody. Tato metoda trasování by měla být použita k záznamu ukončení metod, které vrací celé číslo.

Tato metoda zapíše uživatelskou proceduru do výstupního souboru trasování s odpovídající úrovní odsazení, aby zaznamenala bod, ve kterém tok řízení opouští metodu, a číselný návratový kód z této metody. Tato metoda se používá pouze v případě, že bylo dříve použito volání "entry (String)" v rámci stejné metody.

public void exit (String *fid*, boolean *rc*)

Kde *fid* se používá k identifikaci, kde bylo volání provedeno, například název třídy a metody, a *rc* je logický návratový kód z metody. Tato metoda trasování by měla být použita k záznamu ukončení metod, které vrací logickou hodnotu.

Tato metoda zapíše uživatelskou proceduru do výstupního souboru trasování s odpovídající úrovní odsazení, aby zaznamenala bod, ve kterém tok řízení opouští metodu, a logický návratový kód z této metody. Tato metoda se používá pouze v případě, že bylo dříve použito volání "entry (String)" v rámci stejné metody.

public void data (String *fid*, String data)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody.

Tato metoda zapíše některá řetězcová data do výstupního souboru trasování.

veřejná neobsazená data (String *fid*, int data)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody.

Tato metoda zapíše data typu integer do výstupního souboru trasování.

public void data (String *fid*, byte [])

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody.

Tato metoda zapíše některá binární data do výstupního souboru trasování.

Ukázkové trasování

Chcete-li pomoci diagnostikovat problémy v uživatelské proceduře, můžete použít stejný prostředek trasování jako MQIPT, případně můžete implementovat vlastní funkce trasování. Pokud se rozhodnete použít funkce trasování MQIPT , existují vstupní a výstupní volání, která lze použít při vstupu a výstupu z metody. K dispozici jsou také různá datová volání pro trasování užitečných informací, jak ukazuje následující příklad.

```
/**
* This method is called to initialize the exit (for example, for
* loading validation information) and place itself in a ready
* state to validate connection requests.
*/
 public int init(IPTTrace t) {
 final String fid = "MyExit.init";

 // Trace entry into this method
 t.entry(fid);

 // Trace useful information
 t.data(fid, "Starting exit - MQIPT version " + getVersion());

 // Perform initialization and load any data
 t.data(fid, "Ready for work");

 // Trace exit from this method
 t.exit(fid);

 return ExitRc.OK;
}
```

Tato metoda vytvoří trasování ve formátu zobrazeném v následujícím příkladu:

```
16:36:48.625    14   5000-1s    ------{ ConnectionThread.setCertificateExit()
16:36:48.625    14   5000-1s     Creating instance of certificate exit
16:36:48.625    14   5000-1s     Calling init() of certificate exit
16:36:48.625    14   5000-1s    -------{ MyExit.init()
16:36:48.625    14   5000-1s     Starting exit - MQIPT version 2.1.0.0
16:36:48.625    14   5000-1s    Ready for work
16:36:48.625    14   5000-1s    -------} MyExit.init() rc=0
16:36:48.625    14   5000-1s    ------} ConnectionThread.setCertificateExit() rc=0
```

Návratové kódy ukončení certifikátu v adresáři MQIPT

Návratové kódy, které produkt MQIPT rozpozná při volání uživatelské procedury certifikátu v řadě různých situací

Následující návratové kódy jsou rozpoznány produktem MQIPT při volání uživatelské procedury certifikátu v následujících situacích:

Návratový kód	Popis	Inicializovat	ověřit	Aktualizovat
ExitRc.OK	Požadavek byl úspěšně dokončen.	yes	yes	yes
ExitRc.INIT_CHYBA	Požadavek na init se nezdařil, trasa bude zakázána.	yes		
ExitRc.OBNOVENÍ_CHYBA	Požadavek na aktualizaci se nezdařil, trasa bude zakázána.			yes
ExitRc.VALIDATE_ERROR	Proces ověření se nezdařil, požadavek na připojení byl zamítnut.		yes	
ExitRc.OVĚŘIT_ODMÍTNUTO	Požadavek na ověření platnosti byl odmítnut, požadavek na připojení byl odmítnut.		yes	

LDAP a seznamy CRL v adresáři MQIPT

Produkt MQIPT podporuje použití serveru LDAP (Lightweight Directory Access Protocol) k provádění ověřování seznamu odvolaných certifikátů (CRL) na digitálním certifikátu.

Podpora LDAP byla implementována podobným způsobem jako v produktu IBM MQ, protože stejný server LDAP lze použít jak pro IBM MQ , tak pro MQIPT.

Během navázání komunikace SSL/TLS se komunikující partneři navzájem ověřují pomocí digitálních certifikátů. Ověření může zahrnovat i kontrolu, zda je přijatý certifikát nadále důvěryhodný. Certifikační autority (CA) odvolávají certifikáty z různých důvodů, včetně následujících:

- Vlastník se přesunul do jiné organizace.
- Soukromý klíč již není tajný.

Certifikační autority publikují odvolané osobní certifikáty v seznamu odvolaných certifikátů (CRL). Certifikáty CA, které byly odvolány, jsou publikovány v seznamu odvolaných oprávnění (ARL). Všimněte si, že následné odkazy na seznamy CRL se vztahují také na seznamy ARL.

Další informace o použití serverů LDAP s produktem IBM MQ a o správě seznamů CRL a ARL naleznete v tématu Práce se seznamy odvolaných certifikátů a seznamy odvolaných oprávnění.

Produkt MQIPT může podporovat až dva servery LDAP na každé trase. První server LDAP je považován za hlavní server a druhý server LDAP je uchován jako záloha. Druhý server se používá pouze v případě, že hlavní server není dosažitelný. Záložní server by měl být zrcadlovým obrazem hlavního serveru.

Přístup k informacím uloženým na serveru LDAP lze chránit pomocí ID uživatele a hesla pomocí vlastností ID uživatele a hesla LDAP. Hesla serveru LDAP lze šifrovat v MQIPT konfiguraci z IBM MQ 9.1.5. Další informace o šifrování hesel, která má produkt MQIPTpoužívat, naleznete v části “Šifrování uložených hesel v adresáři MQIPT” na stránce 1046.

Když MQIPT načte token PKCS #12 ze souboru svazku klíčů, všechny certifikáty CA se kontrolují na platnost CRL. Pokud má certifikát CA připojený seznam CRL, je zkontrolováno, zda mu vypršela platnost, a pokud ano, je ze serveru LDAP načten novější seznam CRL. Každý načtený seznam CRL je načten do aktuálního tokenu a připojen k jeho certifikátu CA.

Pokud se při odesílání dotazu na hlavní server LDAP neshodují žádné položky s danou certifikační autoritou, předpokládá se, že pro tuto certifikační autoritu neexistují žádné seznamy CRL a záložní server není použit. Pokud však hlavní server LDAP není dosažitelný nebo se nevrátí v daném časovém rámci, použije se záložní server. Jakékoli chyby ze záložního serveru způsobí ukončení připojení klienta. Tuto akci lze přepsat nastavením vlastnosti **LDAPIgnoreErrors** na hodnotu `true`.

Všechny seznamy CRL načtené produktem MQIPT jsou uloženy v mezipaměti a sdíleny všemi připojeními na dané trase. Pokud vypršela platnost seznamu CRL uloženého v mezipaměti, bude seznam CRL odebrán z mezipaměti a ze serveru LDAP bude načten nový seznam CRL. Pokud není k dispozici nový seznam CRL, připojení je stále odmítnuto.

Seznam CRL načtený ze serveru LDAP je také kontrolován pro vypršení platnosti a zobrazí se varovná zpráva (MQCPW001). Vypršelý seznam CRL je stále zaveden do systému a všechny požadavky na připojení odkazující na tento seznam CRL jsou odmítnuty. Měli byste nahradit seznam CRL s vypršenou platností na serveru LDAP aktuálním seznamem CRL.

Vlastnost **LDAPCacheTimeout** lze použít k řízení toho, jak často je mezipaměť CRL vymazána. Výchozí hodnota je 1 den. Nastavení této hodnoty na `0` znamená, že položky mezipaměti nebudou vymazány, dokud nebude trasa restartována.

Seznam CRL, jehož platnost vypršela, lze uložit do souboru svazku klíčů nebo na server LDAP. Pokud nebyl vydán nový seznam CRL, další požadavky na připojení budou odmítnuty. Vypršelé seznamy CRL můžete ignorovat povolením vlastnosti **IgnoreExpiredCRLs** .

Poznámka: Pokud povolíte vlastnost **LDAPIgnoreErrors** nebo vlastnost **IgnoreExpiredCRLs** , lze k vytvoření připojení SSL/TLS použít zrušený certifikát.

Vlastnosti org. jednotky rozlišujícího názvu certifikátu s více hodnotami v souboru MQIPT

Můžete porovnat více hodnot organizační jednotky (OU) v rozlišujících názvech certifikátů.

Následující vlastnosti trasy nyní podporují shodu více hodnot organizační jednotky:

- **SSLClientDN_OU**
- **SSLClientSiteDN_OU**
- **SSLServerDN_OU**
- **SSLServerSiteDN_OU**

Chcete-li porovnat více hodnot organizační jednotky, použijte čárku jako oddělovač v hodnotě vlastnosti trasy. Příklad:

```
SSLClientDN_OU=Sales, Europe
```

Toto odpovídá certifikátům jak s `OU=Sales` , tak s `OU=Europe`. Hodnoty organizační jednotky se shodují ve stejné posloupnosti jako více hodnot organizační jednotky ve filtrech IBM MQ SSLPEER.

V sekci `[route]` nezadávejte stejnou vlastnost trasy více než jednou. Správným způsobem, jak porovnat více hodnot organizační jednotky, je zadat vlastnost jednou, jak je uvedeno v předchozím příkladu. Pokud zadáte stejný atribut více než jednou ve stejné sekci `mqipt.conf` , poslední hodnota se projeví. Například následující položky by měly za následek pouze shodu s položkou `Evropa` , protože druhý řádek přepíše první řádek:

```
SSLClientDN_OU=Sales
SSLClientDN_OU=Europe
```

Pokud se musíte shodovat s literálovou čárkou uvnitř hodnoty organizační jednotky, vložte zpětné lomítko (\) jako řídicí znak bezprostředně před čárku. Příklad:

```
SSLClientDN_OU=Sales\, Europe
```

Odpovídá jedné hodnotě: `OU=Sales, Europe`. Zpětné lomítko, které není bezprostředně následováno čárkou, odpovídá literálovému zpětnému lomítku.

Pokud provádíte upgrade z předchozí verze produktu MQIPT a spoléháte na schopnost porovnat čárky v hodnotách organizační jednotky, musíte vložit řídicí znaky zpětného lomítka do vlastností trasy organizační jednotky, abyste zachovali předchozí chování.

Deprecated Povolení zamítnutých protokolů a sad šifrování v produktu MQIPT

Standardně jsou protokoly zabezpečených soketů a šifrovací sady, které jsou považovány za nezabezpečené, zakázány v prostředí Java runtime environment (JRE) dodávaném s produktem MQIPT. Tyto zamítnuté protokoly a šifrovací sady musí být před použitím povoleny.

Informace o této úloze

Pokud jste si vědomi potenciálních rizik, ale stále potřebujete použít jeden z protokolů nebo šifrovacích sad, které jsou v produktu MQIPTpovažovány za nezabezpečené, postupujte podle této procedury, abyste povolili protokol nebo šifrovací sadu, kterou potřebujete použít.

Poznámka: Zamítnuté protokoly a šifrovací sady nelze použít s příkazovým portem TLS.

Postup

1. Upravte soubor `java.security` , který se nachází v adresáři *mqipt_path*`/java/jre/lib/security` , kde *mqipt_path* je umístění, kde je nainstalován produkt MQIPT .
2. Přidejte podporu do prostředí JRE pro protokol nebo algoritmus tak, že odeberete odpovídající položku ze seznamu zakázaných algoritmů ve vlastnosti `jdk.tls.disabledAlgorithms` .
   - Chcete-li přidat podporu pro protokol, odeberte protokol ze seznamu zakázaných algoritmů. Chcete-li například přidat podporu pro TLS 1.0, odeberte TLSv1 ze seznamu.
   - Chcete-li přidat podporu pro šifrovací sadu, odeberte odpovídající algoritmy ze seznamu zakázaných algoritmů. Chcete-li například přidat podporu pro šifrovací sadu SSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA , odeberte 3DES_EDE_CBC a DESede ze seznamu.
3. Chcete-li povolit zabezpečení SSL 3.0 v prostředí JRE, musíte také nastavit systémovou vlastnost `com.ibm.jsse2.disableSSLv3=false`.

   Pokud spouštíte produkt MQIPT z příkazového řádku pomocí příkazu **mqipt** , můžete nastavit vlastnost pomocí proměnné prostředí **MQIPT_JVM_OPTIONS**. Příklad:

   ```
   set MQIPT_JVM_OPTIONS=-Dcom.ibm.jsse2.disableSSLv3=false
   ```

   Windows Je-li produkt MQIPT nainstalován jako služba systému Windows , můžete tuto vlastnost nastavit definováním hodnoty řetězce v registru Windows pod klíčem `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MQInternetPassThru` . Hodnota by měla mít následující atributy:

   Název
   Volby MqiptJvm

   Údaje o hodnotě
   -Dcom.ibm.jsse2.disableSSLv3=false
4. Chcete-li povolit SSL 3.0, TLS 1.0nebo TLS 1.1 na přenosové cestě MQIPT , přidejte odpovídající protokol do vlastnosti přenosové cesty **SSLServerProtocols** nebo **SSLClientProtocols** .
5. Restartujte produkt MQIPT , aby se změny vlastností prostředí JRE projevily.

Použití šifrovacího hardwaru PKCS #11 v produktu MQIPT

Produkt MQIPT může přistupovat k digitálním certifikátům uloženým v šifrovacím hardwaru, který podporuje rozhraní PKCS #11 .

Než začnete

Než začnete konfigurovat produkt MQIPT tak, aby používal kryptografický hardware, ujistěte se, že šifrovací karta, ovladač karty a přidružený podpůrný software jsou nainstalovány a řádně fungují.

Podporu šifrovacího hardwaru PKCS #11 v produktu MQIPT poskytuje poskytovatel šifrování IBM Java PKCS11 (poskytovatelIBMPKCS11Impl). Další informace o poskytovateli IBMPKCS11Impl a seznamu

šifrovacích karet podporovaných produktem Java 8naleznete v tématu IBM PKCS11 Poskytovatel šifrování.

Informace o této úloze

Osobní certifikáty a certifikáty CA, ke kterým má produkt MQIPT přístup, můžete uložit do úložiště klíčů šifrovacího hardwaru. Vzhledem k tomu, že zařízení PKCS #11 obvykle nemá k dispozici dostatek místa pro uložení velkého množství certifikátů podepsaného, můžete pro certifikáty CA použít samostatné úložiště klíčů založené na souborech.

Postupujte podle této procedury, chcete-li nakonfigurovat produkt MQIPT tak, aby používal certifikáty v úložišti klíčů šifrovacího hardwaru.

Poznámka: Použití šifrovacího hardwaru s produktem MQIPT je schopnost IBM MQ Advanced . Chcete-li využít tuto schopnost, lokální správce front, který je připojen pomocí přenosové cesty MQIPT , musí mít také nárok IBM MQ Advanced, IBM MQ Appliance, IBM MQ Advanced for z/OS VUEnebo IBM MQ Advanced for z/OS .

Postup

1. Vytvořte konfigurační soubor, který se použije při inicializaci poskytovatele IBMPKCS11Impl .

   Stáhněte si ukázkové konfigurační soubory pro každou hardwarovou šifrovací kartu, kterou podporuje poskytovatel IBMPKCS11Impl , a nakonfigurujte ukázku pro váš systém. Ukázky lze stáhnout z následujícího tématu v souboru IBM Documentation pro Java: Konfigurační soubor.

   Konfigurační soubor je textový soubor a měl by obsahovat alespoň následující atributy:

   Název
   Přípona názvu instance poskytovatele.

   knihovna
   Úplný název knihovny PKCS #11 , která je dodávána s šifrovacím hardwarem.

   tokenlabel
   Popisek tokenu šifrovacího zařízení PKCS #11 .

   Konfigurační soubor může například obsahovat následující položky:

   ```
   name = IPTPKCS11Provider
   library = /usr/lib64/pkcs11/PKCS11_API.so
   tokenlabel = icatoken
   ```

2. Upravte soubor vlastností zabezpečení Java `java.security`umístěný v podadresáři `java/jre/lib/security` instalačního adresáře MQIPT .
   a) Pokud již není v souboru přítomen, přidejte poskytovatele zabezpečení IBMPKCS11Impl .

      Například přidáním následujícího řádku:

      ```
      security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
      ```

   b) Za název poskytovatele přidejte úplný název konfiguračního souboru.

      Pokud se například konfigurační soubor, který jste vytvořili v kroku “1” na stránce 1035 , nazývá `/opt/mqipt/pkcs11.cfg`, měli byste přidat tuto cestu na stejný řádek jako poskytovatel zabezpečení:

      ```
      security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /opt/mqipt/
      pkcs11.cfg
      ```

3. Používáte-li soubor svazku klíčů pro certifikáty CA, vytvořte místo ukládání certifikátů CA v šifrovacím hardwaru soubor svazku klíčů CA ve formátu PKCS #12 .

   Soubor svazku klíčů CA můžete vytvořit buď pomocí grafického uživatelského rozhraní (GUI) systému **mqiptKeyman** , nebo pomocí rozhraní příkazového řádku (CLI) systému **mqiptKeycmd** .

   - Chcete-li použít rozhraní CLI, zadejte tento příkaz:

```
mqiptKeycmd -keydb -create -db filename -pw password -type pkcs12
```

kde *název souboru* je název souboru svazku klíčů, který se má vytvořit, a *heslo* je heslo svazku klíčů.

- Chcete-li použít grafické rozhraní, postupujte takto:
  a. Spusťte grafické rozhraní zadáním příkazu **mqiptKeyman**.
  b. Klepněte na volbu **Soubor databáze klíčů** > **Otevřít**.
  c. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **PKCS11Config**.
  d. Klepněte na tlačítko **OK**. Otevře se okno Otevřít šifrovací token.
  e. Vyberte popisek tokenu šifrovacího zařízení, který chcete použít k uložení certifikátů.
  f. Do pole **Heslo šifrovacího tokenu** zadejte heslo potřebné pro přístup k šifrovacího hardwaru.
  g. Chcete-li vytvořit nový soubor svazku klíčů CA, vyberte volbu **Vytvořit nový sekundární soubor databáze klíčů**.
  h. Klepněte na volbu **Typ databáze klíčů** a vyberte **PKCS12**.
  i. Do pole **Název souboru** zadejte název souboru svazku klíčů CA.
  j. Do pole **Umístění** zadejte úplnou cestu k souboru svazku klíčů CA.
  k. Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.
  l. Zadejte heslo pro svazek klíčů CA do pole **Heslo** a zadejte jej znovu do pole **Potvrdit heslo** .
  m. Klepněte na tlačítko **OK**.

4. Pomocí **mqiptKeycmd** nebo **mqiptKeyman**si vyžádejte osobní certifikát pro kryptografický hardware.
   - Chcete-li použít rozhraní CLI, zadejte tento příkaz:

```
mqiptKeycmd -certreq -create -crypto module_name -tokenlabel hardware_token
            -pw password -label label -size key_size
            -sig_alg algorithm -dn distinguished_name -file filename
```

kde:

-crypto *název_modulu*
Určuje úplný název knihovny PKCS #11 dodávané s šifrovacím hardwarem.

-tokenlabel *token_label*
Určuje popisek tokenu šifrovacího zařízení PKCS #11 .

-pw *heslo*
Určuje heslo pro přístup k kryptografickému hardwaru.

-label *popisek*
Určuje popisek certifikátu.

-size *velikost_klíče*
Určuje velikost klíče. Hodnota může být 512, 1024, 2048nebo 4096.

-sig_alg *algoritmus*
Určuje asymetrický podpisový algoritmus používaný pro vytvoření dvojice klíčů položky. Hodnota může být MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSAnebo SHAWithDSA. Výchozí hodnota je SHA256WithRSA.

-dn *název_rozlišení*
Uvádí rozlišující název X.500 uzavřený v uvozovkách.

-file *název_souboru*
Určuje název souboru pro žádost o certifikát.

- Chcete-li použít grafické rozhraní, postupujte takto:

a. V nabídce **Vytvořit** klepněte na volbu **Nová žádost o certifikát**.

b. Do pole **Popisek klíče** zadejte popisek certifikátu.

c. Vyberte **Velikost klíče** a **Podpisový algoritmus** , který požadujete.

d. Zadejte hodnoty pro **Obecný název** a **Organizaci**a vyberte **Země**. Pro zbývající volitelná pole buď přijměte výchozí hodnoty, nebo zadejte nebo vyberte nové hodnoty.

e. Do pole **Zadejte název souboru, do kterého se má uložit žádost o certifikát** buď přijměte předvolbu `certreq.arm`, nebo zadejte novou hodnotu s úplnou cestou.

f. Klepněte na tlačítko **OK**.

g. Seznam **Požadavky na osobní certifikát** zobrazuje popisek nové žádosti o osobní certifikát, kterou jste vytvořili. Žádost o certifikát je uložena ve vybraném souboru.

5. Poté, co vám CA odešle osobní certifikát, přidejte certifikát CA buď do úložiště šifrovacích klíčů, nebo do souboru svazku klíčů CA, pokud již není přítomen.

   - Chcete-li použít rozhraní příkazového řádku k přidání certifikátu CA do souboru svazku klíčů CA, zadejte následující příkaz:

     ```
     mqiptKeycmd -cert -add -db filename -pw password -type pkcs12
                 -label label -file cert_filename
     ```

     kde *filename* je název souboru svazku klíčů CA, *password* je heslo svazku klíčů CA, *label* je popisek připojený k certifikátu a *cert_filename* je název souboru obsahujícího certifikát CA.

   - Chcete-li použít rozhraní příkazového řádku k přidání certifikátu CA do šifrovacího hardwaru, zadejte následující příkaz:

     ```
     mqiptKeycmd -cert -add -crypto module_name -tokenlabel hardware_token
                 -pw password -label label -file cert_filename
     ```

     kde *název_modulu* je úplný název knihovny PKCS #11 dodávané s šifrovacím hardwarem, *token_hardware_token* je popisek tokenu šifrovacího zařízení PKCS #11 , *heslo* je heslo pro přístup k šifrovacímu hardwaru, *jmenovka* je jmenovka připojená k certifikátu a *název_souboru_certu* je název souboru obsahujícího certifikát CA.

   - Chcete-li použít grafické rozhraní, postupujte takto:

     a. V poli **Obsah databáze klíčů** vyberte položku **Certifikáty podepsaného**.

     b. Klepněte na tlačítko **Přidat**. Otevře se okno Přidat certifikát CA ze souboru.

     c. Zadejte název a umístění souboru certifikátů, v němž je certifikát uložen, nebo klepněte na tlačítko **Procházet** a vyberte soubor a umístění.

     d. Klepněte na tlačítko **OK**. Otevře se okno Zadat jmenovku.

     e. V okně Zadat jmenovku zadejte název certifikátu.

     f. Klepněte na tlačítko **OK**. Dojde k přidání certifikátu do databáze klíčů.

6. Přijměte osobní certifikát poskytnutý certifikační autoritou do úložiště klíčů šifrovacího hardwaru.

   - Chcete-li použít rozhraní CLI, zadejte tento příkaz:

     ```
     mqiptKeycmd -cert -receive -file filename -crypto module_name
                 -tokenlabel hardware_token -pw password
     ```

     kde *název souboru* je název souboru obsahujícího certifikát, který se má přijmout, *název_modulu* je úplný název knihovny PKCS #11 dodané s šifrovacím hardwarem, *token hardware_token* je popisek tokenu šifrovacího zařízení PKCS #11 a *heslo* je heslo pro přístup k šifrovacímu hardwaru.

     Pokud je certifikát CA uložen ve svazku klíčů CA a nikoli v šifrovacím hardwaru, obdržíte varování, že řetěz certifikátů nelze ověřit, protože příkaz **mqiptKeycmd** nemůže přistupovat ke svazku klíčů CA při přijímání osobního certifikátu do úložiště šifrovacích klíčů.

   - Chcete-li použít grafické rozhraní, postupujte takto:

     a. Klepněte na tlačítko **Přijmout**. Otevře se okno Přijmout certifikát ze souboru.

b. Zadejte název souboru certifikátů a umístění nového osobního certifikátu nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.

c. Klepněte na tlačítko **OK**. Pole **Osobní certifikáty** zobrazuje popisek nového osobního certifikátu, který jste přidali.

7. Zašifrujte heslo pro přístup k kryptografickému hardwaru pomocí příkazu **mqiptPW** .

   Zadejte následující příkaz:

   ```
   mqiptPW -sf encryption_key_file
   ```

   kde *soubor_šifrování_klíčů* je název souboru, který obsahuje šifrovací klíč hesla pro vaši instalaci produktu MQIPT . Parametr **-sf** nemusíte zadávat, pokud vaše instalace produktu MQIPT používá výchozí šifrovací klíč hesla. Zadejte heslo pro přístup k šifrovacího hardwaru, který se má šifrovat, když jste vyzváni.

   Další informace o šifrování hesel úložiště klíčů viz “Šifrování hesla svazku klíčů v souboru MQIPT” na stránce 1019.

8. Pokud jste v kroku “3” na stránce 1035vytvořili soubor svazku klíčů CA, zašifrujte heslo pro soubor svazku klíčů CA podle pokynů v kroku “7” na stránce 1038.
9. Upravte konfigurační soubor `mqipt.conf` .
   a) Potvrďte, že máte odpovídající nárok na použití této funkce IBM MQ Advanced , nastavením globální vlastnosti **EnableAdvancedCapabilities** na hodnotu `true`.
   b) Povolte použití úložiště klíčů kryptografického hardwaru na trase nastavením jedné nebo více vlastností **SSLServerKeyRingUseCryptoHardware**, **SSLServerCAKeyRingUseCryptoHardware**, **SSLServerKeyRingUseCryptoHardware**nebo **SSLServerKeyRingUseCryptoHardware** na hodnotu `true`.

      Další informace o vlastnostech, které povolují použití šifrovacího hardwaru na trase, viz MQIPT vlastnosti směrování.

      V produktu IBM MQ 9.2.0můžete také použít šifrovací hardware s portem příkazu TLS nastavením vlastnosti **SSLCommandPortKeyRingUseCryptoHardware** na hodnotu `true`.
   c) Používáte-li soubor svazku klíčů pro certifikáty CA, zadejte umístění svazku klíčů CA nastavením jedné nebo více vlastností **SSLServerCAKeyRing** nebo **SSLServerCAKeyRing** .

      Pokud jste konfigurovali přenosovou cestu pro použití šifrovacího hardwaru pro certifikát serveru a nespecifikujete soubor svazku klíčů CA, použije se úložiště klíčů šifrovacího hardwaru jako úložiště klíčů CA.
   d) Zadejte šifrované heslo pro přístup k šifrovanému hardwaru a svazku klíčů CA pomocí vlastnosti **SSLServerKeyRingPW**, **SSLServerCAKeyRingPW**, **SSLClientKeyRingPW**, **SSLClientCAKeyRingPW**nebo **SSLCommandPortKeyRingPW** .

      Nastavte hodnotu vlastností **SSL*KeyRingPW** na výstup šifrovaného hesla pomocí příkazu **mqiptPW** .
   e) Pokud šifrovací hardware obsahuje více než jeden osobní certifikát, uveďte, který certifikát by měl být vybrán produktem MQIPT pro odeslání na server SSL/TLS nebo klienta pro ověření.

      Můžete určit, který certifikát by měl být vybrán, nastavením jedné nebo více vlastností **SSLClientSite*** pro trasu klienta SSL/TLS nebo jedné z vlastností **SSLServerSite*** pro trasu serveru SSL/TLS.

      Můžete určit, který certifikát by měl být používán příkazovým portem TLS, pomocí vlastnosti **SSLCommandPortSiteLabel** k určení názvu popisku certifikátu.

      Další informace o výběru certifikátů ze svazku klíčů viz “Výběr certifikátů ze souboru svazku klíčů v adresáři MQIPT” na stránce 1019. Vlastnosti pro výběr certifikátu ze svazku klíčů jsou popsány v části MQIPT vlastnosti směrování.

   Chcete-li například použít úložiště klíčů kryptografického hardwaru pro certifikát serveru na trase serveru TLS a soubor svazku klíčů pro uložení certifikátů CA pro stejnou trasu, přidejte do definice trasy následující vlastnosti:

```
SSLServerKeyRingUseCryptoHardware=true
SSLServerKeyRingPW=<mqiptPW>1!gORdM4wft5d1rCgNMDEGag==!dZxhgQD2A8Ea0yeqawQvPg==
SSLServerCAKeyRing=/opt/mqipt/ssl/ca.pfx
SSLServerCAKeyRingPW=<mqiptPW>1!3Vdrpiu6kMwn0sWRCVgT5g==!LHltGLEg3OFvN8+02Re0YA==
SSLServerSiteLabel=mqiptsite
```

10. Restartujte produkt MQIPT.

Java security managervstup MQIPT

Funkci Java security manager lze použít s libovolnou funkcí MQIPT , která poskytuje další úroveň zabezpečení.

Poznámka: Deprecated Použití Java security manager s MQIPT je zamítnuto, protože Java security manager bylo zamítnuto pro odebrání v budoucí verzi produktu Java.

MQIPT používá výchozí Java security manager , jak je definováno ve třídě `java.lang.SecurityManager` . Funkci Java security manager v produktu MQIPT lze povolit nebo zakázat pomocí globální vlastnosti **SecurityManager**. Další informace viz MQIPT globální vlastnosti .

Java security manager používá dva výchozí soubory zásad:

- Globální soubor zásad systému s názvem *$MQIPT_PATH*`/java/jre/lib/security/java.policy` (kde *$MQIPT_PATH* je adresář, kde je nainstalován produkt MQIPT) je používán všemi instancemi virtuálního počítače na hostiteli.
- Soubor zásad specifický pro uživatele s názvem `.java.policy`, který může existovat v domovském adresáři uživatele.

Lze také použít další soubor zásad MQIPT . Místo dříve popsaných výchozích souborů zásad byste měli použít soubor zásad MQIPT . Další informace viz **SecurityManagerPolicy** v části MQIPT globální vlastnosti .

Syntaxe souboru zásad je poměrně složitá a i když ji lze změnit pomocí textového editoru, je obvykle jednodušší použít obslužný program Policy Tool poskytovaný s produktem Java pro provedení změn. Obslužný program Policy Tool se nachází v adresáři *$MQIPT_PATH*`/java/jre/bin` a je plně zdokumentován v dokumentaci Java.

Ukázkový soubor zásad (`mqiptSample.policy`) byl poskytnut s produktem MQIPT , aby vám ukázal, jaká oprávnění musí být nastavena pro spuštění produktu MQIPT.

Musíte upravit ukázkový soubor zásad tak, aby odpovídal vaší konfiguraci. Všimněte si zejména, že domovský adresář MQIPT , který obsahuje konfigurační soubor `mqipt.conf` , nemusí být stejný jako instalační adresář MQIPT , proto při konfiguraci položek **FilePermission** v zásadě zabezpečení dávejte pozor na uvedení správných adresářů.

Musíte změnit následující položky:

- Položka **java.io.FilePermission** , která uděluje přístup pro `čtení` a `zápis` k adresáři `errors` . Cesta k souboru v této položce musí odkazovat na domovský adresář MQIPT , protože zde je umístěn adresář `errors` . Produkt MQIPT vytvoří soubory FFST Failure Data Capture files (`AMQ*.FDC`) a trasovací soubory (`AMQ*.TRC*`) v adresáři `errors` . Musíte se ujistit, že produkt MQIPT má oprávnění k vytváření souborů trasování a souborů FFST v adresáři `errors` , aby bylo možné odstraňování problémů.
- Položka **java.io.FilePermission** , která uděluje přístup pro `čtení` a `zápis` k adresáři `logs` . Cesta k souboru v této položce musí odkazovat na domovský adresář MQIPT , protože zde je umístěn adresář `logs` . Produkt MQIPT vytvoří soubory protokolu připojení (`mqipt*.log`) v adresáři `logs` , pokud je povolena globální vlastnost **ConnectionLog** .
- Položky **java.io.FilePermission** , které udělují přístup `read` a `execute` k libovolným adresářům v instalačním adresáři MQIPT , jako jsou adresáře `bin`, `exits`, `liba` `ssl` . Cesty k souborům v těchto položkách musí být změněny tak, aby odkazovaly na instalační adresář MQIPT . Některé z těchto položek mohou být vynechány, pokud nejsou požadovány.

- Položky **java.net.SocketPermission** musí být upraveny tak, aby řídily připojení ke každé trase MQIPT naslouchání. Oprávnění `listen` a `accept` jsou požadována pro port modulu listener a adresu modulu listener pro každou trasu MQIPT .
- Položky **java.net.SocketPermission** musí být upraveny tak, aby řídily připojení mimo každou trasu MQIPT . Oprávnění `connect` je vyžadováno pro všechna místa určení trasy, servery proxy nebo servery LDAP, ke kterým se připojuje trasa MQIPT . Oprávnění `resolve` je vyžadováno při zadávání cílů pomocí názvu hostitele místo adresy IP.

V závislosti na konfiguraci budete možná muset přidat následující položky:

- Položka **java.io.FilePermission** pro udělení přístupu pro čtení ke konfiguračnímu souboru `mqipt.conf` nebo k domovskému adresáři MQIPT obsahujícímu `mqipt.conf`.
- Položka **java.io.FilePermission** pro udělení přístupu pro čtení k samotnému souboru zásad zabezpečení. To je užitečné, pokud aktualizace MQIPT způsobí, že soubor zásad zabezpečení bude znovu načten.
- Některé položky **java.io.FilePermission** pro udělení přístupu pro čtení k libovolným souborům svazku klíčů SSL/TLS a souborům hesel svazku klíčů. Toto je vyžadováno pouze při použití přenosové cesty, která má povolené vlastnosti **SSLClient** nebo **SSLServer** , nebo při konfiguraci příkazového portu TLS.
- Některé položky **java.io.FilePermission** , kterým se má udělit přístup `read` nebo `execute` k libovolným uživatelským třídám MQIPT . Tato volba je vyžadována pouze v případě, že je povolena uživatelská procedura MQIPT . Možná budete muset udělit další oprávnění, pokud to uživatelská procedura vyžaduje.

Poznámka: Položky Windows **java.io.FilePermission** musí používat dvě zpětná lomítka (\\) pro každé zpětné lomítko v cestě. Důvodem je, že jako řídicí znak se používá jedno zpětné lomítko.

Ukázkový soubor předpokládá, že byl produkt MQIPT nainstalován na systému Windows v adresáři `C:\Program Files\IBM\MQ Internet Pass-Thru`. Také předpokládá, že domovský adresář MQIPT (umístění souboru `mqipt.conf`) je stejný jako instalační adresář MQIPT .

Pokud jste nainstalovali produkt MQIPT do jiného umístění, musíte změnit adresář v definici **codeBase** tak, aby odkazoval na váš instalační adresář MQIPT . Dávejte pozor, abyste zahrnuli správnou předponu (`file:/`) a správnou příponu souboru (`/lib/com.ibm.mq.ipt.jar`). Na systémech AIX and Linux může být typická **codeBase** URL `file:/opt/mqipt/lib/com.ibm.mq.ipt.jar`, za předpokladu, že MQIPT je nainstalován v adresáři `/opt/mqipt`.

Oprávnění jsou obvykle definována se třemi atributy. Chcete-li řídit připojení soketů, jejich hodnoty jsou:

oprávnění ke třídám
`java.net.SocketPermission`

název, který se má řídit
Tento formát je tvořen formátem `hostname:port`, kde lze každou komponentu názvu zadat pomocí zástupného znaku. Název hostitele může být název domény nebo adresa IP. Pozici názvu hostitele, která je nejvíce vlevo, lze zadat hvězdičkou (*). Například `harry.company1.com` by se shodovalo s každým z těchto řetězců:

- `harry`
- `harry.company1.com`
- `*.company1.com`
- `*`
- `198.51.100.123` (za předpokladu, že se jedná o adresu IP `harry.company1.com`)

Komponenta portu názvu může být uvedena jako jedna adresa portu nebo rozsah adres portů, například:

1414
pouze port 1414

1414-V roce
všechny adresy portů větší nebo rovny 1414

-1414
všechny adresy portů menší nebo rovny 1414

1-1414
všechny adresy portů mezi 1 a 1414 včetně

povolená akce
Akce používané produktem `java.net.SocketPermission` jsou:

Přijmout
Povolit přijetí připojení z určeného cíle

connect
Povolit připojení k určenému cíli

Naslouchá
Povolit aplikaci naslouchat na uvedeném portu nebo portech pro požadavky na připojení

Vyřešit
Povolit použití DNS pro překlad názvů domén na adresy IP

Ovládací prvek Java security manager lze také provést prostřednictvím systémových vlastností `java.security.manager` a `java.security.policy` Java , ale doporučuje se použít vlastnosti **SecurityManager** a **SecurityManagerPolicy** pro řízení MQIPT.

Chcete-li zahrnout diagnostické informace do záznamů trasování a FFST , MQIPT musí přistupovat k určitým systémovým vlastnostem a proměnným prostředí MQIPT . V zásadě zabezpečení Java musíte vždy zahrnout následující vlastnosti:

```
permission java.util.PropertyPermission "java.home", "read";
permission java.util.PropertyPermission "java.version", "read";
permission java.util.PropertyPermission "java.runtime.version", "read";
permission java.util.PropertyPermission "java.vm.info", "read";
permission java.util.PropertyPermission "java.vm.vendor", "read";
permission java.util.PropertyPermission "os.arch", "read";
permission java.util.PropertyPermission "os.name", "read";
permission java.util.PropertyPermission "os.version", "read";
permission java.lang.RuntimePermission "getenv.MQIPT_PATH";
permission java.lang.RuntimePermission "getStackTrace";
permission javax.management.MBeanServerPermission "createMBeanServer";
permission javax.management.MBeanPermission "com.ibm.mq.ipt.IPTManager#-
[com.ibm.mq.ipt:type=IPTManager]", "registerMBean";
permission javax.management.MBeanPermission "com.ibm.mq.ipt.IPTManager#-
[com.ibm.mq.ipt:type=IPTManager]", "unregisterMBean";
permission javax.management.MBeanTrustPermission "register";
```

Pokud nezahrnete všechny tyto vlastnosti, produkt MQIPT nebude správně fungovat a diagnostika problému bude narušena.

Uživatelské procedury zabezpečení v adresáři MQIPT

Pomocí uživatelské procedury zabezpečení můžete řídit přístup k cílovému místu určení, jak je definováno vlastností trasy **Destination** . Uživatelská procedura zabezpečení je volána v okamžiku, kdy produkt MQIPT obdrží od klienta požadavek na připojení, ale předtím, než vytvoří připojení k cílovému místu určení.

Na základě počátečních vlastností připojení rozhoduje uživatelská procedura zabezpečení, zda je povoleno připojení dokončit.

Při spuštění přenosové cesty je volána uživatelská procedura zabezpečení, aby se inicializovala a připravila ke zpracování požadavku na připojení. Inicializační proces by měl být použit k načtení jakýchkoli uživatelských dat a připravit tato data pro rychlý a snadný přístup, čímž se minimalizuje doba potřebná ke zpracování požadavku na připojení.

Každá přenosová cesta může mít svou vlastní uživatelskou proceduru zabezpečení.

- Vlastnost **SecurityExit** se používá k povolení/zakázání uživatelské procedury zabezpečení definované uživatelem.
- Vlastnost **SecurityExitName** se používá k definování názvu třídy uživatelské procedury zabezpečení definované uživatelem.
- Vlastnost **SecurityExitPath** se používá k definování názvu adresáře obsahujícího soubor třídy. Není-li tato vlastnost nastavena, předpokládá se, že soubor třídy bude nalezen v podadresáři exits. **SecurityExitPath** může také definovat název souboru JAR obsahujícího uživatelskou proceduru pro zabezpečení zprávy definovanou uživatelem.
- Vlastnost **SecurityExitTimeout** používá produkt MQIPT k určení, jak dlouho má čekat na odezvu z uživatelské procedury zabezpečení při ověřování požadavku na připojení.

Podrobnosti o vlastnostech uživatelské procedury zabezpečení naleznete v tématu MQIPT Vlastnosti směrování .

Produkt MQIPT používá třídu `SecurityExit` k volání uživatelské procedury zabezpečení definované uživatelem. Tato třída musí být rozšířena uživatelskou procedurou pro zabezpečení zprávy definovanou uživatelem a většina jejích metod musí být potlačena, aby poskytovala požadovanou funkčnost. Objekt `SecurityExitResponse` se používá k zpětnému předání dat do produktu MQIPT a tato data používá produkt MQIPT k rozhodnutí, zda má být požadavek na připojení přijat nebo odmítnut. Objekt `SecurityExitResponse` může také obsahovat novou adresu cílového a cílového portu, která se používá k přepsání přenosové cesty definované vlastnostmi uživatelské procedury zabezpečení.

K dispozici jsou tři ukázkové uživatelské procedury zabezpečení, které vám ukážou, jak lze implementovat uživatelskou proceduru zabezpečení.

- `SampleSecurityExit` ukazuje, jak řídit přístup ke správci front IBM MQ na základě názvu kanálu IBM MQ . Umožňuje pouze připojení s názvem kanálu začínajícím řetězcem "MQIPT." Další informace naleznete v tématu Použití uživatelské procedury zabezpečení .
- Produkt `SampleRoutingExit` umožňuje dynamické směrování požadavků na připojení klienta do fondu definovaných serverů IBM MQ , přičemž každý server je hostitelem správce front se stejným názvem a stejnými atributy. Ukázka obsahuje konfigurační soubor, který obsahuje seznam názvů serverů. Další informace naleznete v tématu Směrování požadavků na připojení klienta k serverům správce front IBM MQ pomocí uživatelských procedur zabezpečení .
- Produkt `SampleOneRouteExit` umožňuje dynamické směrování na správce front IBM MQ , který je odvozen od názvu kanálu IBM MQ použitého v požadavku na připojení. Ukázka obsahuje konfigurační soubor, který obsahuje mapování názvů správců front na názvy serverů. Další informace naleznete v tématu Dynamické směrování požadavků na připojení klienta .

Poznámka: Produkt MQIPT se spouští v jednom prostředí JVM, takže uživatelská procedura zabezpečení může ohrozit normální provoz produktu MQIPT jedním z těchto způsobů:

- Ovlivnit systémové prostředky
- Generovat kritická místa
- Snížit výkon

Před implementací do produkčního prostředí byste měli důkladně otestovat účinky uživatelské procedury zabezpečení.

Třída com.ibm.mq.ipt.exit.SecurityExit v souboru MQIPT

Tato třída a její veřejné metody musí být rozšířeny uživatelskou procedurou pro zabezpečení, aby získala přístup k některým obecným datům a umožnila určitou MQIPT inicializaci.

Před voláním každé metody produktem MQIPTbudou některé vlastnosti zpřístupněny pro metodu, která má být použita. Jejich hodnoty lze načíst pomocí příslušných metod get definovaných v této třídě.

metody

public int init (IPTTrace) (veřejná vnitřní inicializace)
K dispozici jsou následující vlastnosti:

- port modulu listener
- cíl
- Cílový port
- verze

Metoda `init` je volána produktem MQIPT při spuštění přenosové cesty. Při návratu z této metody musí být uživatelská procedura zabezpečení připravena ověřit požadavek na připojení. Platné návratové kódy jsou `ExitRc.OK` nebo `ExitRc.INIT_ERROR`.

public int refresh (IPTTrace) (veřejná obnova int)
K dispozici jsou následující vlastnosti:

- port modulu listener
- cíl
- Cílový port

Metoda `refresh` je volána produktem MQIPT při aktualizaci konfigurace MQIPT . Tato akce se obvykle provádí, když byla v konfiguračním souboru změněna vlastnost. Produkt MQIPT znovu načte všechny vlastnosti z konfiguračního souboru, aby určil, které vlastnosti byly změněny a zda je třeba restartovat trasu.

Tato metoda by měla provést opětovné načtení všech externích dat, která používá; tj. dat načtených metodou **`init`** . Platné návratové kódy jsou `ExitRc.OK` nebo `ExitRc.REFRESH_ERROR`.

public void close (IPTTrace) (veřejné anulování)
K dispozici jsou následující vlastnosti:

- port modulu listener
- cíl
- Cílový port

Metoda `close` je volána produktem MQIPT , když se zastavuje. Tato metoda by měla uvolnit všechny systémové prostředky, které uživatelská procedura získala během své činnosti. Produkt MQIPT čeká na dokončení této metody před ukončením.

Tato metoda je také volána, pokud byla dříve povolena uživatelská procedura zabezpečení, ale nyní byla zakázána v konfiguračním souboru.

public SecurityExitOvěření odezvy (IPTTrace)
K dispozici jsou následující vlastnosti:

- port modulu listener
- cíl
- Cílový port
- časový limit
- Adresa IP klienta
- adresa portu klienta
- Název kanálu
- Název správce front

Metoda `validate` je volána produktem MQIPT , když obdrží požadavek na připojení k ověření. Název kanálu a název správce front nebudou k dispozici, pokud byla povolena vlastnost **`SSLProxyMode`** , protože tato funkce se používá pouze k tunelování dat TLS, a proto jsou data obvykle získaná z počátečního datového toku nečitelná.

Uživatelská procedura zabezpečení musí vrátit objekt `SecurityExitResponse` obsahující následující informace:

- kód příčiny (musí být nastaven)
- nová cílová adresa (nepovinné)

- nová adresa portu cílového modulu listener (volitelné)
- zpráva (nepovinné)

Kód příčiny určuje, zda je připojení přijato nebo odmítnuto produktem MQIPT. Pole `newDestination` a `newDestinationPort` lze volitelně nastavit tak, aby definovala nového cílového správce front. Pokud tyto vlastnosti nenastavíte, použijí se vlastnosti směrování **`Destination`** a **`DestinationPort`** definované v konfiguračním souboru. Jakákoli vrácená zpráva je připojena k položce souboru protokolu připojení.

Pro získání hodnot vlastností konfigurace MQIPT jsou podporovány následující metody:

public int getListenerPort () (
načte port modulu listener trasy-jak je definováno vlastností **`ListenerPort`**

public String getDestination()
načte cílovou adresu-jak je definováno vlastností **`Destination`**

public int getDestinationPort ()
načte adresu portu cílového modulu listener-jak je definováno vlastností **`DestinationPort`**

veřejný řetězec getClientIPAddress ()
načte adresu IP klienta, který vytváří požadavek na připojení

public int getClientPortAddress()
načte adresu portu používanou klientem, který zadává požadavek na připojení

public int getTimeout()
načte hodnotu časového limitu. MQIPT bude čekat na uživatelskou proceduru pro zabezpečení zprávy, aby ověřila požadavek-jak je definováno vlastností **`SecurityExitTimeout`**

public int getConnThreadID()
načte ID podprocesu připojení, který zpracovává požadavek na připojení, což je užitečné pro účely ladění

veřejný řetězec getChannelname ()
načte název kanálu IBM MQ použitý v požadavku na připojení

public String getQMName()
načte název správce front IBM MQ použitý v požadavku na připojení

public boolean getTimedout()
může být použit uživatelskou procedurou pro zabezpečení zprávy k určení, zda vypršel časový limit

Třída com.ibm.mq.ipt.exit.SecurityExitResponse v souboru MQIPT

Tato třída se používá k předání odezvy zpět do produktu MQIPT z uživatelské procedury pro zabezpečení zprávy definované uživatelem a používá se k určení, zda má být požadavek na připojení přijat nebo odmítnut.

Objekty tohoto typu jsou vytvářeny pouze v metodě ověření (viz "Třída com.ibm.mq.ipt.exit.SecurityExit v souboru MQIPT" na stránce 1042). Existují konstruktory pro usnadnění vytváření těchto objektů a existují metody pro každou vlastnost. Další informace naleznete v ukázkových uživatelských procedur zabezpečení.

Vytvoření výchozího objektu odezvy SecurityExitodmítne požadavek na připojení.

Konstruktory

- **public SecurityExitResponse (String dest, int destPort, int rc, String msg)**

  kde:

  - `dest` je nové cílové místo určení.
  - `destPort` je nová adresa cílového portu
  - `rc` je kód příčiny
  - `msg` je zpráva, která bude přidána do položky protokolu připojení.

- **public SecurityExitResponse (String dest, int destPort, int rc)**
- **public SecurityExitOdezva (int rc, String msg)**
- **public SecurityExitOdezva (int rc)**

metody

public void setDestination(String dest)
nastaví novou cílovou adresu pro požadavek na připojení

public void setDestinationPort (int port) vyvolá výjimku IPTException
nastaví novou adresu cílového portu modulu listener pro požadavek na připojení-vyvolá výjimku IPTException pro neplatnou adresu portu

public void setMessage(String msg)
přidá zprávu do záznamu protokolu připojení

public void setReasonKód (int rc)
nastaví kód příčiny pro požadavek na připojení.

Návratové kódy uživatelské procedury zabezpečení v adresáři MQIPT

Návratové kódy, které produkt MQIPT rozpozná při volání uživatelské procedury pro zabezpečení zprávy v řadě různých situací.

Následující návratové kódy jsou rozpoznány produktem MQIPT při volání uživatelské procedury zabezpečení v následujících situacích:

Návratový kód	Popis	Inicializovat	ověřit	Aktualizovat
ExitRc.OK	Požadavek byl úspěšně dokončen.	yes	yes	yes
ExitRc.INIT_CHYBA	Požadavek na init se nezdařil, trasa bude zakázána.	yes		
ExitRc.OBNOVENÍ_CHYBA	Požadavek na aktualizaci se nezdařil.			yes
ExitRc.NEAUTORIZOVÁNO	Proces ověření se nezdařil, požadavek na připojení byl zamítnut.		yes	
ExitRc.DISABLE_SSL	Požadavek na ověření byl úspěšný, připojení k cíli nebude používat SSL nebo TLS.		yes	

Ovládací prvek čísla portu v adresáři MQIPT

Při použití MQIPTje možné omezit rozsah čísel lokálních portů, které se používají při vytváření odchozího připojení.

Nastavte vlastnost **OutgoingPort** na trase, abyste zadali počáteční číslo lokálního portu, a nastavte **MaxConnectionThreads** , abyste uvedli počet portů, které se mají použít. Pokud například nastavíte **OutgoingPort** na 1600 a **MaxConnectionThreads** na 20, bude rozsah čísel lokálních portů pro tuto trasu 1600-1619.

Je odpovědností administrátora produktu MQIPT , aby se ujistil, že mezi trasami nejsou žádné konflikty čísel portů.

Není-li parametr **OutgoingPort** definován, výchozí hodnota 0 znamená, že se pro každé připojení použije číslo portu přidělené systémem.

Při použití HTTPje počet odchozích portů dvojnásobný, když nepoužíváte HTTP. V předchozím příkladu, pokud přenosová cesta použila HTTP, rozsah čísel bude 1600-1639.

Další informace viz Přidělení čísel portů .

Multihomed systémy

Používáte-li systém s více adresami, můžete pomocí vlastnosti **LocalAddress** určit, ke které adrese IP bude navázáno odchozí připojení. Názvy hostitelů nejsou v této vlastnosti podporovány.

Šifrování uložených hesel v adresáři MQIPT

Konfigurace produktu MQIPT může zahrnovat hesla pro přístup k různým prostředkům a také heslo pro přístup k produktu MQIPT pomocí příkazového portu. Z produktu IBM MQ 9.2.0by všechna tato hesla měla být chráněna šifrováním.

Informace o této úloze

Ve verzích starších než IBM MQ 9.2.0lze šifrovat pouze hesla, která používá produkt MQIPT pro přístup ke klíčům nebo úložištím klíčů šifrovacího hardwaru. Šifrovaná hesla jsou uložena v souborech, na které odkazuje kterákoli z vlastností **SSL*KeyRingPW** . Ostatní hesla pro servery LDAP a heslo pro přístup MQIPT jsou uložena v prostém textu v konfiguračním souboru `mqipt.conf` .

V systému IBM MQ 9.2.0by všechna uložená hesla pro použití produktem MQIPT měla být chráněna šifrováním hesla pomocí příkazu **mqiptPW** . Šifrovaná hesla jsou uložena jako hodnoty vlastností v konfiguračním souboru `mqipt.conf` . Produkt MQIPT je schopen rozlišovat mezi zašifrovanými hesly, hesly v prostém textu a názvy souborů v hodnotách vlastností. Měli byste zašifrovat všechna hesla uložená pro použití produktem MQIPT tímto způsobem, protože se jedná o nejbezpečnější metodu ochrany.

Deprecated Metoda šifrování hesel úložiště klíčů použitá v produktu MQIPT před IBM MQ 9.2.0 je zamítnutá, ale stále ji lze použít pro vlastnosti konfigurace, které byly k dispozici před produktem IBM MQ 9.2.0. Chcete-li zlepšit ochranu hesel klíčového řetězce, znovu zašifrujte všechna hesla klíčového řetězce, která byla dříve zašifrována, pomocí nejnovější metody ochrany.

Poznámka: Vlastnost **SSLCommandPortKeyRingPW** v konfiguračním souboru `mqipt.conf` a vlastnost **SSLClientCAKeyRingPW** v souboru vlastností **mqiptAdmin** nemohou odkazovat na soubory hesel. Hodnoty těchto vlastností musí být nastaveny na šifrovaný řetězcový výstup hesla příkazem **mqiptPW** .

Pokud je v konfiguraci produktu MQIPT uveden prostý text nebo slabě chráněné heslo, je vydána varovná zpráva buď při spuštění produktu MQIPT , nebo při spuštění trasy.

Pomocí této procedury zašifrujte heslo, které má být uloženo pro použití produktem MQIPT pomocí nejnovější metody ochrany. Chcete-li zašifrovat heslo svazku klíčů v MQIPT před IBM MQ 9.2.0, postupujte podle kroků v části “Šifrování hesla svazku klíčů před MQIPT v IBM MQ 9.2.0” na stránce 1047.

Postup

1. Volitelné: Vytvořte soubor obsahující šifrovací klíč hesla, pokud jej ještě nemáte.

   Produkt MQIPT používá k šifrování hesel šifrovací klíč. V souboru můžete zadat vlastní šifrovací klíč. Soubor musí obsahovat alespoň jeden znak a pouze jeden řádek textu.

   Stejný šifrovací klíč hesla se používá k šifrování a dešifrování všech uložených hesel pro instanci produktu MQIPT. Proto potřebujete pro každou instalaci produktu MQIPT pouze jeden soubor s šifrovacími klíči hesla.

   K šifrování hesel uložených v souboru vlastností **mqiptAdmin** můžete použít jiný šifrovací klíč hesla než šifrovací klíč použitý k šifrování hesel v konfiguraci produktu MQIPT .

   Pokud plánujete spustit produkt MQIPT jako službu, která se spustí automaticky, musíte vytvořit soubor s šifrovacím klíčem hesla s výchozím názvem `mqipt_cred.keya` umístit jej do domovského adresáře MQIPT .

   Nemusíte zadávat šifrovací klíč hesla, ale je to bezpečnější. Pokud neuvedete vlastní šifrovací klíč, použije se výchozí šifrovací klíč.

Poznámka: Musíte se ujistit, že jsou v souboru s klíči šifrování hesla nastavena příslušná oprávnění k souboru, abyste zabránili neoprávněným uživatelům ve čtení šifrovacího klíče. Pouze uživatel, který spustil příkaz **mqiptPW** , a uživatel, pod kterým je spuštěn produkt MQIPT , potřebují oprávnění ke čtení šifrovacího klíče hesla.

2. Zašifrujte heslo pomocí příkazu **mqiptPW** .

   Syntaxe příkazu **mqiptPW** je popsána v části mqiptPW (šifrovat uložené heslo).

   Pokud jste v kroku “1” na stránce 1046vytvořili soubor s šifrovacími klíči hesla, zadejte název souboru pomocí parametru **-sf** pro **mqiptPW**. Například lze zadat následující příkaz k zašifrování hesla pomocí šifrovacího klíče v souboru určeném parametrem **-sf** :

   ```
   mqiptPW -sf /opt/mqipt/mqipt_password.key
   ```

3. Zadejte heslo, které má být šifrováno, když jste vyzváni.

   Šifrované heslo bude výstupem **mqiptPW**.

4. Zkopírujte šifrované heslo do příslušné vlastnosti v konfiguračním souboru `mqipt.conf` nebo v souboru vlastností **mqiptAdmin** .

   Například následující řádek uvádí šifrované heslo pro přístupové heslo MQIPT :

   ```
   AccessPW=<mqiptPW>1!QL+2Jvj/tigKKlD7Nz8Oqw==!AMDBefOUrmPf5i1OuqV5MA==
   ```

5. Spusťte produkt MQIPT. Pokud jste v kroku “1” na stránce 1046 vytvořili soubor s šifrovacím klíčem hesla s jiným než výchozím názvem, zadejte při spouštění souboru MQIPTnázev souboru s šifrovacím klíčem.

   Můžete uvést název souboru s klíči šifrování hesla pomocí parametru **-sf** při spuštění MQIPT. Chcete-li například spustit příkaz MQIPT pomocí šifrovacího klíče v souboru určeném parametrem **-sf** , zadejte tento příkaz:

   ```
   mqipt /opt/mqipt -sf /opt/mqipt/mqipt_password.key
   ```

   Informace o dalších metodách zadání názvu souboru s klíči šifrování hesla při spuštění produktu MQIPTnaleznete v tématu Zadání šifrovacího klíče hesla.

   Název souboru s klíči šifrování hesla pro příkaz **mqiptAdmin** můžete zadat pomocí vlastnosti **PasswordProtectionKeyFile** v souboru vlastností **mqiptAdmin** .

Šifrování hesla svazku klíčů před MQIPT v IBM MQ 9.2.0

Před produktem IBM MQ 9.2.0jsou šifrovaná hesla, která se používají pro přístup ke klíčům používaným produktem MQIPT , uložena v souborech.

Informace o této úloze

Postupujte podle procedury v této úloze, abyste zašifrovali heslo svazku klíčů pro použití MQIPT před IBM MQ 9.2.0. V části MQIPT v části IBM MQ 9.2.0 for Long Term Supportpoužijte bezpečnější metodu ochrany popsanou v části “Šifrování uložených hesel v adresáři MQIPT” na stránce 1046.

Postup

1. Zašifrujte heslo svazku klíčů pomocí příkazu **mqiptPW** .

   Zadejte následující příkaz k zašifrování hesla:

   ```
   mqiptPW password filename
   ```

   kde:

   Password
   je heslo pro čistý text potřebné pro přístup ke svazku klíčů

Filename
je název souboru hesel, který se má vytvořit

Syntaxe příkazu **mqiptPW** je popsána v části mqiptPW (šifrovat uložené heslo).

2. Nastavte odpovídající vlastnost směrování na název souboru, který obsahuje šifrované heslo vytvořené v kroku “1” na stránce 1047.

   Chcete-li například zadat soubor hesel pro svazek klíčů, který obsahuje certifikát serveru MQIPT TLS, přidejte do konfiguračního souboru `mqipt.conf` následující řádek:

   ```
   SSLServerKeyRingPW=filename
   ```

Další aspekty zabezpečení pro produkt MQIPT

Produkt MQIPT má několik dalších funkcí, které návrháři pomáhají sestavit zabezpečené řešení.

- Je-li v interní síti mnoho klientů, kteří se všichni pokoušejí vytvořit odchozí připojení, mohou všichni projít přes server MQIPT umístěný uvnitř brány firewall. Administrátor brány firewall pak musí udělit externí přístup pouze k počítači MQIPT .
- Produkt MQIPT se může připojit pouze ke správcům front, pro které byl explicitně nakonfigurován ve svém konfiguračním souboru, pokud produkt MQIPT nejedná jako server proxy SOCKS nebo nepoužívá uživatelskou proceduru zabezpečení.
- Produkt MQIPT ověřuje, zda jsou zprávy, které přijímá a přenáší, platné a zda jsou v souladu s protokolem IBM MQ . To pomáhá zabránit tomu, aby byl produkt MQIPT používán pro bezpečnostní útoky mimo protokol IBM MQ . Pokud produkt MQIPT vystupuje jako server proxy SSL/TLS a všechna data a protokoly IBM MQ byly šifrovány, může produkt MQIPT zaručit pouze počáteční navázání komunikace SSL/TLS. V této situaci použijte Java security manager.
- Produkt MQIPT umožňuje kanálovým exitům spouštět vlastní komplexní protokoly zabezpečení.
- Nastavením vlastnosti `MaxConnectionThreads` můžete omezit celkový počet příchozích připojení. To pomáhá chránit zranitelného interního správce front před útoky typu odepření služby.

Konfigurační soubor

Konfigurační soubor MQIPT , `mqipt.conf`, musíte chránit před čtením neautorizovanými uživateli, protože může obsahovat citlivé informace, jako např. heslo **AccessPW** , které řídí vzdálený administrativní přístup k produktu MQIPT. Ochraňte všechna hesla uvedená v konfiguračním souboru podle procedury uvedené v části “Šifrování uložených hesel v adresáři MQIPT” na stránce 1046. Také se ujistěte, že je produkt `mqipt.conf` chráněn proti neoprávněným úpravám. Nastavte oprávnění k souboru operačního systému pro systém `mqipt.conf` tak, aby soubor mohl číst nebo aktualizovat pouze uživatelský účet, který spouští produkt MQIPT .

Příkazový port

Příkazové porty MQIPT přijímají administrativní příkazy vydané přes síť pro vzdálenou instanci produktu MQIPT příkazem **mqiptAdmin** .

V produktu IBM MQ 9.2.0lze MQIPT konfigurovat jeden nezabezpečený příkazový port a jeden příkazový port zabezpečený pomocí protokolu TLS. Připojení k nezabezpečenému příkazovému portu nejsou šifrována.

Poznámka: Data odeslaná po síti na nezabezpečený příkazový port, včetně přístupového hesla MQIPT , mohou být viditelná pro ostatní uživatele v síti.

Před povolením nezabezpečeného příkazového portu nebo portu TLS je třeba zvážit, zda je třeba povolit příkazový port, a posoudit rizika povolení vzdálené administrace produktu MQIPT. V produktu IBM MQ 9.2.0může příkaz **mqiptAdmin** spravovat lokální instance produktu MQIPT , které jsou spuštěny pod stejným uživatelem jako příkaz **mqiptAdmin** , bez použití příkazového portu. Proto možná nebudete muset povolit příkazový port pro správu lokálních instancí produktu MQIPT.

Je-li povolen nezabezpečený příkazový port nebo port TLS, musíte zabránit neoprávněnému přístupu k příkazovému portu. Při zabezpečení přístupu k příkazovému portu byste například měli zvážit tyto body:

- Pomocí brány firewall můžete omezit sadu počítačů, které se mohou připojit k příkazovému portu MQIPT .
- Povolte ověření na příkazových portech pomocí vlastností **AccessPW** a **RemoteCommandAuthentication** . Další informace o povolení ověřování příkazového portu naleznete v tématu Ověřování příkazového portu.
- Zvažte zakázání vzdáleného vypnutí pomocí vlastnosti **RemoteShutdown** .
- Zvažte použití vlastností **CommandPortListenerAddress** a **SSLCommandPortListenerAddress** ke konfiguraci příkazových portů pro naslouchání na specifickém síťovém rozhraní.

Další informace o použití příkazu **mqiptAdmin** k administraci MQIPTnaleznete v tématu Administrace MQIPT pomocí příkazového řádku.

Protokoly připojení v adresáři MQIPT

Produkt MQIPT poskytuje prostředek protokolu připojení, který obsahuje seznam všech úspěšných a neúspěšných pokusů o připojení.

Záznam se zapíše do protokolu připojení pro každé připojení přijaté nebo vytvořené přenosovou cestou MQIPT a pro každý administrativní příkaz přijatý produktem MQIPT. Protokol připojení je řízen pomocí vlastností **ConnectionLog** a **MaxLogFileSize** . Další informace viz MQIPT globální vlastnosti .

Při každém spuštění produktu MQIPT se vytvoří nový protokol připojení. Pro identifikaci název souboru obsahuje aktuální časové razítko, například:

```
mqiptYYYYMMDDHHmmSS.log
```

kde:

YYYY je rok
MM je měsíc
DD je den.
HH je počet hodin
mm jsou minuty
SS je počet sekund

Když protokol připojení dosáhne maximální velikosti určené vlastností **MaxLogFileSize** , vytvoří se záložní soubor `mqipt001.log`. Udržují se maximálně dva záložní soubory (`mqipt001.log` a `mqipt002.log`).

Položka v protokolu připojení představuje každou část požadavku na připojení. Požadavek na připojení přijatý produktem MQIPT a výsledné nové připojení, které produkt MQIPT vytvoří k cílové adrese, se zobrazí jako dvě položky protokolu a následně po ukončení každého připojení dvě další položky.

Zde je protokol připojení pro úspěšný požadavek na připojení:

```
Wed May 15 13:13:51 BST 2013 conn accept 127.0.0.1(3842) 127.0.0.1(5000) OK 5000-0
Wed May 15 13:13:51 BST 2013 conn conn   127.0.0.1(3843) localhost(3500) OK 5000-0
Wed May 15 13:13:52 BST 2013 conn close  127.0.0.1(3842) 127.0.0.1(5000) OK 5000-0
Wed May 15 13:13:52 BST 2013 conn close  127.0.0.1(3843) localhost(3500) OK 5000-0
```

Zde je protokol připojení pro nezdařený požadavek na připojení:

```
Wed May 15 14:56:40 BST 2013 conn accept 127.0.0.1(4138) 127.0.0.1(7000) OK    7000-0
Wed May 15 14:56:40 BST 2013 conn close  127.0.0.1(4138) 127.0.0.1(7000) ERROR 7000-0
 Unrecognized SSL handshake request '54'
```

Položky protokolu připojení

Každá položka protokolu připojení obsahuje následující informace:

- Čas, kdy byla položka vytvořena.
- Typ položky. Hodnota může být jedna z následujících hodnot:

  admin
  Administrativní příkaz

  připojení
  Připojení přenosové cesty
- Událost, ke které došlo. Hodnota může být jedna z následujících hodnot:

  Přijmout
  Přijat požadavek na připojení

  zavřít
  Připojení je zavřené

  připojení
  Požadavek na připojení k cíli trasy

  Živec
  Přijat příkaz Display MQIPT

  nodata
  Od volajícího nebyla přijata žádná data

  ping
  Přijat požadavek na příkaz ping

  stav
  Přijat příkaz pro zobrazení stavu

  refr
  Byl přijat příkaz refresh

  zastavit
  Přijat příkaz k zastavení
- Zdrojová síťová adresa a číslo portu. Hodnota LOCAL se zobrazí pro administrativní příkazy vydané lokálně bez použití příkazového portu.
- Cílová síťová adresa a číslo portu. Toto není zobrazeno pro administrativní příkazy vydané lokálně bez použití příkazového portu.
- Kód dokončení. Hodnota může být OK nebo ERROR.
- Identifikátor podprocesu MQIPT .
- Volitelná chybová zpráva.

Konfigurace produktu IBM MQ Internet Pass-Thru pomocí kontejnerů

IBM MQ Internet Pass-Thru (MQIPT) můžete spustit v kontejneru. Základní obraz použitý kontejnerovým obrazem musí používat podporovaný operační systém Linux.

Procedura

- Ukázkový obraz produktu MQIPT Docker je k dispozici v úložišti GitHub kontejneru mq. Chcete-li sestavit a spustit kontejner, postupujte podle pokynů v tématu IBM MQ Internet Pass-Thru na webu Docker.

Jak pokračovat dále

Spuštěné kontejnery můžete zobrazit pomocí příkazu **docker ps** . Chcete-li zobrazit výstup konzoly MQIPT spuštěného v kontejneru Docker , použijte příkaz **docker logs ${CONTAINER_ID}** .

V 9.3.0 Konfigurace kontinuálních front

Funkce proudových front vám umožňuje mít duplicitní kopii každé zprávy vloženou do fronty, doručenou do druhé fronty. Konfigurace datových proudů front se provádí ve frontě podle fronty.

Lokální a modelové fronty mají dva nové atributy související s frontami proudu:

STREAMQ
Jedná se o název fronty, do které mají být doručeny zprávy s kontinuální relací. Atribut **STREAMQ** byste měli nastavit na název jiné fronty.

Existují omezení, pro která lze fronty konfigurovat tak, aby proudily zprávy do jiných front, a existují omezení, pro která lze fronty nastavit jako místo určení pro proudové zprávy. Informace o omezeních proudu zpráv viz Omezení fronty proudů.

STRMQOS
Jedná se o kvalitu služby, která se má použít při doručování streamovaných zpráv.

Atribut **STRMQOS** můžete nastavit na jednu ze dvou hodnot:

BESTEF
Nejlepší úsilí, což je výchozí hodnota.

Správce front se pokusí doručit kopii každé zprávy do fronty určené v atributu **STREAMQ** . Pokud se vyskytl problém s doručením zprávy, neovlivní to doručení původní zprávy.

MUSTDUP
Správce front se pokusí doručit kopii každé zprávy do fronty proudu.

Pokud se vyskytl problém s doručením zprávy se streamem, původní zpráva se nedoručí do fronty a aplikace obdrží MQCC_FAILED spolu s odpovídajícím kódem příčiny.

Další podrobnosti viz příkazy ALTER queues, DEFINE queues a DISPLAY QUEUE MQSC a příkazy Change, Copy a Create Queue, Inquire Queue a Inquire Queue (Response) PCF.

Pokud je požadována více než jedna kopie každé zprávy, můžete nakonfigurovat atribut **STREAMQ** tak, aby odkazoval na název alias fronty IBM MQ , jejíž cíl odkazuje na téma IBM MQ . Když je zpráva vložena do původní fronty, je kopie zprávy publikována do uvedeného tématu.

Musíte se ujistit, že máte rozhraní API nebo spravované odběry objektu tématu, protože každý odběr obdrží kopii zprávy. Zpráva doručená odběratelům se řídí stejnými pravidly jako ostatní zprávy publikování/odběru. Například každá zpráva má nový identifikátor zprávy a pole kontextu MQMD se liší od polí v původní zprávě. Další informace o podobnostech a rozdílech mezi původními a proudovými zprávami viz Streamované zprávy.

Příklady

Příklad nejlepšího úsilí

V následujícím příkladu se jedná o lokální frontu ORDERS.QUEUE je pozměněna tak, aby vkládaly proudové zprávy do druhé fronty ANALYTICS.QUEUE. Kvalita služby BESTEF se používá k zajištění toho, že v případě problému s vložením zprávy s proudovou službou do produktu ANALYTICS.QUEUE, například pokud je to ANALYTICS.QUEUE je plná, původní zprávu lze přesto vložit do ORDERS.QUEUE.

Tento typ konfigurace lze použít k provedení analýzy přijímaných objednávek pomocí analýzy streamovaných zpráv, zatímco původní zprávy jsou vloženy do fronty objednávek a zpracovány. Výhodou funkce proudové fronty je, že můžete zanechat streamované zprávy v produktu ANALYTICS.QUEUE čeká na zpracování, aniž by to ovlivnilo skutečné objednávky, které podnik uspokojuje.

```
DEFINE QLOCAL(ANALYTICS.QUEUE)

ALTER QLOCAL(ORDERS.QUEUE) STRMQOS(BESTEF) STREAMQ(ANALYTICS.QUEUE)
```

Poznámka: V příkladu byl parametr **STRMQOS** nastaven na hodnotu BESTEF, ačkoli tento atribut můžete vynechat z příkazu **ALTER** , protože BESTEF je výchozí kvalitou služby.

Je třeba duplikovat příklad

V tomto příkladu lokální fronta PAYMENTS.QUEUE je pozměněna tak, aby vložila kopie všech zpráv do jiné lokální fronty AUDIT.QUEUE. Je důležité, aby každá zpráva vložená do platební fronty byla streamována do fronty auditu, takže se použije kvalita služby MUSTDUP.

Pokud se vyskytl problém s doručením zprávy s kontinuální zprávou do fronty, původní zpráva se nedoručí a aplikace obdrží vhodné dokončení a kód příčiny. Aplikace se musí znovu pokusit o vložení stejným způsobem, jakým by to bylo v případě, že by se jednalo pouze o jedinou frontu.

```
DEFINE QLOCAL(AUDIT.QUEUE)

ALTER QLOCAL(PAYMENTS.QUEUE) STRMQOS(MUSTDUP) STREAMQ(AUDIT.QUEUE)
```

Notes:

1. Při změně původní fronty není nutné, aby fronta proudu existovala. Je však důležité si uvědomit, že vzhledem k tomu, že kvalita používané služby je MUSTDUP, pokusy o vložení zpráv do původní fronty selžou, dokud nedefinujete frontu proudu.
2. Používáte-li alias fronty s cílem objektu tématu a nejsou-li žádní odběratelé, je doručení streamované zprávy stále považováno za úspěšné a původní zpráva je doručena do fronty.
3. Pokud zprávu s kontinuální relací nelze doručit do své fronty, správce front se ji nepokusí doručit do fronty nedoručených zpráv. Je-li však proudová zpráva odeslána do vzdálené fronty a prochází-li kanálem do jiného správce front, může být doručena do fronty nedoručených zpráv v souladu s existujícími pravidly nedoručených zpráv.

Konfigurace fronty proudu

V proudové frontě není třeba provádět žádnou další konfiguraci. Přijímá zprávy ze všech front, které ji pojmenují jako proudovou frontu. Může však být rozumné vzít v úvahu hodnoty atributů nakonfigurované v proudové frontě.

Má-li například původní fronta maximální hloubku 100 000 a proudová fronta má maximální hloubku pouze 5 000, mohou být při nastavení parametru STRMQOS na hodnotu BESTEF ztraceny proudové zprávy, nebo pokud je parametr STRMQOS nastaven na hodnotu MUSTDUP při chybě MQRC_Q_FULL, i když je v původní frontě dostatek místa.

Zvažte, které atributy ve frontě proudu by mohly být změněny, aby měly odpovídající hodnoty, na základě toho, jak je konfigurována původní fronta.

Související pojmy

Fronty proudu

Poznámky

Tyto informace byly vyvinuty pro produkty a služby poskytované v USA.

Společnost IBM nemusí nabízet produkty, služby nebo funkce uvedené v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou ve vaší oblasti aktuálně dostupné, získáte od místního zástupce společnosti IBM. Odkazy na produkty, programy nebo služby společnosti IBM v této publikaci nejsou míněny jako vyjádření nutnosti použití pouze uvedených produktů, programů či služeb společnosti IBM. Místo toho lze použít jakýkoli funkčně ekvivalentní produkt, program nebo službu, které neporušují žádná práva k duševnímu vlastnictví IBM. Ověření funkčnosti produktu, programu nebo služby pocházející od jiného výrobce je však povinností uživatele.

Společnost IBM může vlastnit patenty nebo nevyřízené žádosti o patenty zahrnující předměty popsané v tomto dokumentu. Vlastnictví tohoto dokumentu neposkytuje licenci k těmto patentům. Dotazy týkající se licencí můžete posílat písemně na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Odpovědi na dotazy týkající se licencí pro dvoubajtové znakové sady (DBCS) získáte od oddělení IBM Intellectual Property Department ve vaší zemi, nebo tyto dotazy můžete zasílat písemně na adresu:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Následující odstavec se netýká Spojeného království ani jiných zemí, ve kterých je takovéto vyjádření v rozporu s místními zákony: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE "TAK, JAK JE" BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás toto omezení nemusí vztahovat.

Uvedené údaje mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené jsou pravidelně upravovány a tyto změny budou zahrnuty v nových vydáních této publikace. Společnost IBM může kdykoli bez upozornění provádět vylepšení nebo změny v produktech či programech popsaných v této publikaci.

Veškeré uvedené odkazy na webové stránky, které nespravuje společnost IBM, jsou uváděny pouze pro referenci a v žádném případě neslouží jako záruka funkčnosti těchto webů. Materiály uvedené na tomto webu nejsou součástí materiálů pro tento produkt IBM a použití uvedených stránek je pouze na vlastní nebezpečí.

Společnost IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vyžádání vašeho svolení.

Vlastníci licence k tomuto programu, kteří chtějí získat informace o možnostech (i) výměny informací s nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) oboustranného využití vyměňovaných informací, mohou kontaktovat informační středisko na adrese:

IBM Corporation
Koordinátor interoperability softwaru, oddělení 49XA
3605 Dálnice 52 N

Rochester, MN 55901
U.S.A.

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

Licencovaný program popsaný v těchto informacích a veškerý licencovaný materiál, který je pro něj k dispozici, jsou poskytovány společností IBM na základě podmínek IBM Smlouvy se zákazníkem, IBM Mezinárodní licenční smlouvy pro programy nebo jiné ekvivalentní smlouvy mezi námi.

Jakékoli údaje o výkonnosti obsažené v této publikaci byly zjištěny v řízeném prostředí. Výsledky získané v jakémkoli jiném operačním prostředí se proto mohou výrazně lišit. Některá měření mohla být prováděna na vývojových verzích systémů a není zaručeno, že tato měření budou stejná i na běžně dostupných systémech. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky mohou být jiné. Čtenáři tohoto dokumentu by měli zjistit použitelné údaje pro své specifické prostředí.

Informace týkající se produktů jiných výrobců pocházejí od dodavatelů těchto produktů, z jejich veřejných oznámení nebo z jiných veřejně dostupných zdrojů. Společnost IBM tyto produkty netestovala a nemůže potvrdit správný výkon, kompatibilitu ani žádné jiné výroky týkající se produktů jiných výrobců než IBM. Otázky týkající se kompatibility produktů jiných výrobců by měly být směrovány dodavatelům těchto produktů.

Veškerá tvrzení týkající se budoucího směru vývoje nebo záměrů společnosti IBM se mohou bez upozornění změnit nebo mohou být zrušena a reprezentují pouze cíle a plány společnosti.

Tyto údaje obsahují příklady dat a sestav používaných v běžných obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob a názvy společností, značek a produktů. Všechna tato jména a názvy jsou fiktivní a jejich podobnost se jmény, názvy a adresami používanými ve skutečnosti je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly plně testovány za všech podmínek. Společnost IBM proto nemůže zaručit spolehlivost, upotřebitelnost nebo funkčnost těchto programů.

Při prohlížení těchto dokumentů v elektronické podobě se nemusí zobrazit všechny fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Informace o programovacím rozhraní, jsou-li poskytnuty, jsou určeny k tomu, aby vám pomohly vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, která zákazníkům umožňují psát programy za účelem získání služeb produktu WebSphere MQ.

Tyto informace však mohou obsahovat i diagnostické údaje a informace o úpravách a ladění. Informace o diagnostice, úpravách a vyladění jsou poskytovány jako podpora ladění softwarových aplikací.

Důležité: Tyto informace o diagnostice, úpravách a ladění nepoužívejte jako programovací rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM , ibm.com, jsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek společnosti IBM je k dispozici na webu "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Další názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností.

Microsoft a Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Tento produkt zahrnuje software vyvinutý projektem Eclipse (https://www.eclipse.org/).

Java a všechny ochranné známky a loga založené na termínu Java jsou ochranné známky nebo registrované ochranné známky společnosti Oracle anebo příbuzných společností.

Číslo položky:

(1P) P/N: