9.1

Konfigurace produktu IBM MQ

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 981.

Toto vydání se vztahuje k verzi 9 vydání 1 produktu IBM® MQ a ke všem následujícím vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak.

Obsah

Konfigurace produktu IBM MQ

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

Informace o této úloze

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

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

Pokyny, jak vytvořit, spustit, zastavit a odstranit správce front, naleznete v tématu “Vytvoření správců front na více platformách” na stránce 7.

Informace o tom, jak vytvořit komponenty potřebné k propojení vašich instalací a aplikací produktu IBM MQ , najdete v tématu “Konfigurace distribuovaných front” na stránce 171.

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

Pokyny pro konfiguraci klastru správců front naleznete v tématu “Konfigurace klastru správce front” na stránce 265.

Chování produktu IBM MQ nebo správce front můžete změnit změnou konfiguračních informací. Další informace viz téma “Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 81. Obecně není třeba restartovat správce front, aby se změny konfigurace projevily, kromě případu, kdy je uvedena v této dokumentaci k produktu.

z/OS Pokyny pro konfiguraci prostoru IBM MQ for z/OSnaleznete v příručce “Konfigurace správců front v systému z/OS” na stránce 795.

Související pojmy

IBM MQ Technický přehled

Související úlohy

Správa lokálních objektů produktu IBM MQ

Správa vzdálených objektů produktu IBM MQ

IBM i Správa produktu IBMi

z/OS Správa serveruIBM MQ for z/OS

Naplánování

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

“Konfigurace správců front v systému z/OS” na stránce 795
Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Multi Vytvoření správců front na více platformách

Než budete moci používat zprávy a fronty, musíte vytvořit a spustit alespoň jednoho správce front a jeho přidružené objekty. Správce front spravuje prostředky, které jsou k ní přidruženy, zejména fronty, které vlastní. Poskytuje aplikacím pro volání rozhraní MQI (Message Queuing Interface) volání příkazů a příkazy k vytvoření, úpravě, zobrazení a odstranění objektů IBM MQ .

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.

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

Instalace přidružená ke správci front
Chcete-li vytvořit správce front, použijte řídicí příkaz IBM MQ **crtmqm**. Příkaz **crtmqm** automaticky asociuje správce front s instalací, ze které byl příkaz **crtmqm** zadán. Pro příkazy, které pracují se správcem front, je třeba zadat příkaz z instalace přidružené ke správci front. Pomocí příkazu setmqm můžete změnit přidruženou instalaci správce front. Všimněte si, že instalační program produktu Windows nepřidává uživatele, který provádí instalaci do skupiny mqm, další podrobnosti viz Oprávnění ke správě produktu IBM MQ v systému UNIX, Linux®, and Windows.

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

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

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

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

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

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

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

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

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

Změna výchozí správy fronty může ovlivnit ostatní uživatele nebo aplikace. Změna nemá žádný vliv na aktuálně připojené aplikace, protože je může použít v rámci původního volání MQI v rámci dalších volání MQI. Tento manipulátor zajišťuje, aby byla volání směrována do stejného správce front. Veškeré aplikace, které se připojují *po* , změnily jste výchozí připojení správce front k novému výchozímu

správci front. To může být to, co jste zamýšleli, ale měli byste to vzít v úvahu, dříve než změníte předvolbu.

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

Určit frontu nedoručených zpráv

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

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

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

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

Při vytváření správce front je třeba pomocí parametru **-u** zadat název fronty nedoručených zpráv. Příkaz MQSC můžete také použít ke změně atributů správce front, kterého jste již definovali, pro určení fronty nedoručených zpráv, která má být použita. Příklad příkazu MQSC ALTER naleznete v tématu Zobrazení a změna atributů správce front .

Určit výchozí přenosovou frontu

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

Při vytváření správce front je třeba pomocí parametru **-d** zadat název výchozí přenosové fronty. Ve skutečnosti to ve skutečnosti nevytvoří frontu; musíte to udělat výslovně později. Další informace naleznete v tématu Práce s lokálními frontami .

Uveďte parametry protokolování, které požadujete

Můžete uvést parametry protokolování v příkazu `crtmqm` , včetně typu protokolování, a cesty a velikosti souborů protokolu.

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

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

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

Další informace o parametrech protokolování viz "Konfigurace vysoké dostupnosti, zotavení a restartu" na stránce 418.

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

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

Informace o této úloze

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

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

Pokud jste vytvořili správce front a jeho objekty, můžete ke spuštění správce front použít příkaz **strmqm** .

Procedura

- Další informace, které vám pomohou při vytváření a správě správců front, naleznete v následujících dílčích tématech:
  - “Vytvoření výchozího správce front” na stránce 11
  - “Nastavení výchozího správce front jako výchozího správce front” 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 81
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 795
Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Související odkazy

Systémové a výchozí objekty

crtmqm

Linux UNIX V 9.1.3 Konfigurovatelný dočasný adresář

IBM MQ 9.1.3 dále obsahuje koncept konfigurovatelného dočasného adresáře, který definuje umístění, do kterého by měla data správce front být pomíjivá. To lze použít k umožnění umístění soketů domény UNIX and Linux na nepřipojený systém souborů v prostředí Red Hat® OpenShift® .

Před IBM MQ 9.1.3na platformách UNIX and Linux je při spuštění správce front UNIX and Linux doménových soketů vytvořeno v adresáři `/var/mqm/sockets` .

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 určitým procesům mimo kontejner kolidovat s operacemi uvnitř kontejneru.

Tento problém zabraňuje spuštění produktu IBM MQ v rámci platformy kontejneru produktu Red Hat OpenShift v rámci výchozího kontextu zabezpečení.

Z produktu IBM MQ 9.1.3lze atribut **EphemeralPrefix** použít ke konfiguraci umístění pomíjivého adresáře. Pokud tento atribut nepoužijete, nebude se zobrazovat žádná změna chování.

Je-li položka správce front vytvořena v produktu `mqs.ini` (pomocí příkazů **crtmqm** nebo **addmqinf**), je přidán atribut **EphemeralPrefix** , pokud:

- Nastavte atribut **DefaultEphemeralPrefix** ve stanze AllQueueManagers .
- Nastavte proměnnou prostředí MQ_EPHEMERAL_PREFIX.

- Uveďte **-v** *EphemeralPrefix* pouze pro příkaz **addmqinf** .

Můžete také explicitně přidat atribut **EphemeralPrefix** do existujícího správce front, když je zastaven, a to je přidáno při restartu správce front.

Pokud zadáte **EphemeralPrefix**, pak při spuštění správce front způsobí, že data pomíjející data správce front budou vytvořena pod touto předponou namísto jejího obvyklého umístění. To znamená:

- Soubory soketů obvykle přítomné pod `/var/mqm/sockets/<QM>` budou nyní pod `/<EphemeralPrefix>/sockets/<QM>`
- Soubory dílčího fondu, které se obvykle nacházejí pod `/<Prefix>/qmgrs/<QM>/@<Subpool>` , nyní budou pod `/<EphemeralPrefix>/qmgrs/<QM>/@<Subpool>`

Notes:

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

Na platformách UNIX and Linux je **EphemeralPrefix** omezeno na 12 znaků.

Zadáte-li **EphemeralPrefix** , která je příliš dlouhá nebo neexistuje, obdržíte zprávu AMQ7001E: `Umístění zadané pro správce front není platné.`

Multi V 9.1.5 Adresář uživatelských dat

IBM MQ 9.1.5 má adresář `userdata` , který můžete použít k ukládání stavu trvalé aplikace.

Každý správce front produktu IBM MQ má vyhrazený systém souborů pro svůj trvalý stav, který obsahuje jak data fronty, tak i protokol zotavení. Systém souborů obsahuje adresář `userdata` , který lze použít k ukládání trvalých stavových informací pro vaše aplikace. Viz Obsah adresáře v systémech Unix a Linux a Obsah adresáře v systémech Windows.

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

- V konfiguracích RDQM tak, aby se informace o aplikaci také pohybovala, když správce front překoná selhání na jiný uzel (viz “Uložení stavu trvalé aplikace” na stránce 528).
- Pro správce front s více instancemi je jejich aplikační stav umístěn spolu s daty správce front v systému souborů sdílené sítě.
- Obecněji platí, že v aplikacích jsou nakonfigurovány služby správce front.

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

Adresář `userdata` má uživatele mqm a skupiny vlastníků a je to světově čitelný, takže uživatelé mohou k němu přistupovat, aniž by museli být ve skupině administrátorů produktu IBM MQ (to znamená mqm). Nemůžete upravit oprávnění k adresáři `userdata` , ale můžete v něm vytvořit obsah s libovolným vlastnictvím a oprávněními, které vyžadujete.

Multi Vytvoření výchozího správce front

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

Než začnete

Před vytvořením výchozího správce front si přečtěte informace popsané v tématu “Vytvoření správců front na více platformách” na stránce 7.

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

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

Informace o této úloze

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

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

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

Další informace o příkazu **crtmqm** a jeho syntaxi naleznete v tématu **crtmqm**.

Procedura

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

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

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

  kde:

  -q
  Označuje, že tento správce front je výchozím správcem front.

  -d MY.DEFAULT.XMIT.QUEUE
  Představuje název výchozí přenosové fronty, kterou má tento správce front použít.

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

  -u SYSTEM.DEAD.LETTER.QUEUE
  Název výchozí fronty pro dead-letter vytvořeného produktem IBM MQ při instalaci.

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

Jak pokračovat dále

Pokud jste vytvořili správce front a jeho objekty, použijte příkaz **strmqm** pro spuštění správce front.

Související pojmy

Práce s lokálními frontami

Související úlohy

“Zálohování konfiguračních souborů po vytvoření správce front” na stránce 14

Konfigurační informace produktu IBM MQ jsou uloženy v konfiguračních souborech v systému UNIX, Linux, and Windows. Po vytvoření správce front zazálohujte své konfigurační soubory. Pokud pak vytvoříte jiného správce front, který způsobuje problémy, můžete zálohy obnovit, až odeberete zdroj daného problému.

Zobrazení a změna atributů správce front

Související odkazy

Systémové a výchozí objekty

Multi Nastavení výchozího správce front jako výchozího správce front

Existující správce front můžete vytvořit jako výchozího správce front ručně pomocí textového editoru nebo v produktu Windows a Linuxpomocí produktu IBM MQ Explorer.

Informace o této úloze

Chcete-li použít textový editor k vytvoření existujícího správce front jako výchozího správce front, postupujte takto.

Windows Linux Pokud v systémech Windows a Linux (platformyx86 a x86-64) dáváte přednost použití produktu IBM MQ Explorer za účelem provedení této změny, prostudujte si téma “Použití příkazu IBM MQ Explorer k vytvoření výchozího správce front” na stránce 13.

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

Procedura

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

Související úlohy

“Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 81
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 příkazu IBM MQ Explorer k vytvoření výchozího správce front

V systémech Windows a Linux (platformyx86 a x86-64) můžete použít produkt IBM MQ Explorer k vytvoření existujícího správce front jako výchozího správce front.

Informace o této úloze

Chcete-li pomocí produktu IBM MQ Explorer vytvořit existujícího správce front jako výchozího správce front v systémech Windows a Linux (platformyx86 a x86-64), postupujte podle následujících kroků.

Dáváte-li přednost použití textového editoru k ručnímu provedení této změny, přečtěte si téma “Nastavení výchozího správce front jako výchozího správce front” na stránce 13.

Postup

1. Otevřete produkt IBM MQ Explorer.
2. Klepněte pravým tlačítkem myši na **IBM MQ**a pak vyberte **Vlastnosti ...**. Zobrazí se panel **Vlastnosti pro produkt IBM MQ** .
3. Do pole **Výchozí název správce front** zadejte název výchozího správce front.

4. Klepněte na tlačítko **OK**.

ULW Zálohování konfiguračních souborů po vytvoření správce front

Konfigurační informace produktu IBM MQ jsou uloženy v konfiguračních souborech v systému UNIX, Linux, and Windows. Po vytvoření správce front zazálohujte své konfigurační soubory. Pokud pak vytvoříte jiného správce front, který způsobuje problémy, můžete zálohy obnovit, až odeberete zdroj daného problému.

Informace o této úloze

Obecně platí, že při každém vytvoření nového správce front zálohujte své konfigurační soubory.

Existují dva typy konfiguračního souboru:

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

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

- Windows Na systémech Windows : `amqp_win.properties`
- Linux UNIX V systémech UNIX a Linux : `amqp_unix.properties`

Související úlohy

“Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 81
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 produktu IBM MQ” na stránce 601
Můžete ochránit správce front proti možné korupci způsobené selháním hardwaru tím, že zálohujete správce front a data správce front tak, že zálohujete pouze konfiguraci správce front a použijete záložní 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 “Který 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 143
Klienty konfigurujete 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 60
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

Který typ komunikace použít

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

Typy přenosového protokolu pro kanály MQI

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

- TCP/IP
- LU 6.2
- NetBIOS
- SPX

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

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

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

Notes:

1. V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Viz Definování Aspera gateway připojení na Linux.
2. Kromě Linux (platforma POWER)

Související pojmy

“Definování připojení TCP na systému Windows” na stránce 231
Definujte připojení TCP nakonfigurováním kanálu na odesílajícím konci, abyste určili adresu cíle, a spuštěním programu modulu listener na přijímajícím konci.

“Definování připojení TCP na systému UNIX and Linux” na stránce 238
Definice kanálu na odesílajícím konci uvádí adresu cíle. Modul listener nebo démon inet je konfigurován pro připojení na konci příjmu.

“Definování připojení TCP na systému IBM i” na stránce 258
V rámci definice kanálu můžete definovat připojení TCP pomocí pole Název připojení.

“Definování připojení TCP na systému z/OS” na stránce 892
Chcete-li definovat připojení TCP, je zde několik nastavení, které je třeba nakonfigurovat.

“Definování připojení LU 6.2 na systému Windows” na stránce 233
Musí být konfigurována služba SNA, aby bylo možné mezi těmito dvěma počítači vytvořit konverzaci LU 6.2 .

“Definování připojení LU 6.2 na systému UNIX and Linux” na stránce 242
Musí být konfigurována služba SNA, aby bylo možné mezi těmito dvěma počítači vytvořit konverzaci LU 6.2 .

“Definování připojení LU 6.2 na systému IBM i” na stránce 260
Definujte podrobnosti o komunikaci LU 6.2 pomocí názvu režimu, názvu TP a názvu připojení pro plně kvalifikované připojení LU 6.2 .

“Definování připojení NetBIOS v systému Windows” na stránce 234

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

Související úlohy

“Definování připojení Aspera gateway v systému Linux” na stránce 757
Produkt IBM Aspera fasp.io Gateway poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě IBM MQ. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux.

Související odkazy

“limity připojení TCP/IP” na stránce 17
Počet neprovedených požadavků na připojení, které lze zařadit do fronty v jednom portu TCP/IP, závisí na platformě. Pokud je dosažen limit, dojde k chybě.

“Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS” na stránce 894
Chcete-li definovat připojení LU6.2 , je třeba nakonfigurovat několik nastavení.

limity připojení TCP/IP

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

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

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

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

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

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

Konfigurace rozšířeného transakčního klienta

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

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

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

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

WebSphere Application Server
Dřívější verze produktu IBM WebSphere MQ podporovaly WebSphere Application Server 4 nebo 5 a vyžadovaly, abyste provedli určité konfigurační úlohy, abyste mohli používat rozšířeného transakčního klienta. Produkt WebSphere Application Server 6 a dále obsahuje poskytovatele systému zpráv IBM WebSphere MQ nebo IBM MQ , takže nemusíte používat rozšířeného transakčního klienta.

Konfigurace správců transakcí s podporou standardu XA

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

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

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

- 

Instalace klienta IBM MQ v systému AIX
- 

Instalace klienta IBM MQ v systému Linux
- 

Instalace klienta IBM MQ v systému Solaris
- 

Instalace klienta IBM MQ v systému Windows
- 

Instalace klienta IBM MQ v systému IBM i

Pomocí informací pro vaši platformu můžete nakonfigurovat rozšířenou transakční funkci pro správce transakcí kompatibilní se standardem XA, jako je CICS a Tuxedo.

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

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

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

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

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

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

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

- Řetězec xa_open
- Ukazatel na strukturu přepínačů XA

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

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

Formát řetězce xa_open a další informace o tom, jak jsou informace v řetězci xa_open použity rozšířeným transakčním klientem, viz “Formát řetězce xa_open” na stránce 20.

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

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

- “Konfigurace rozšířeného transakčního klienta pro produkt CICS” na stránce 25
- “Konfigurace rozšířeného transakčního klienta pro Tuxedo” na stránce 27

Související pojmy

“Parametry CHANNEL, TRPTYPE, CONNAME a QMNAME řetězce xa_open” na stránce 22
Tyto informace vám pomohou pochopit, jak rozšířený transakční klient používá tyto parametry k určení správce front, k němuž se má připojit.

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

Související úlohy

“Použití rozšířeného transakčního klienta s kanály TLS” na stránce 25
Není možné nastavit kanál TLS pomocí řetězce xa_open. Postupujte podle těchto pokynů, chcete-li použít tabulku definic kanálů klienta (ccdt).

Související odkazy

“Parametry TPM a AXLIB” na stránce 23
Rozšířený transakční klient používá parametry TPM a AXLIB k vyhledání funkcí ax_reg a ax_unreg správce transakcí. Tyto funkce se používají pouze v případě, že správce front používá dynamickou registraci.

“Zotavení po selhání v rozšířeném transakčního zpracování” na stránce 24
Po selhání musí být správce transakcí schopen obnovit všechny nekompletní jednotky práce. Aby to bylo možné provést, správce transakcí musí být schopen otevřít správce front správce front, který se účastnil nedokončené transakce v době selhání.

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

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

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

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

Jiným příkladem je, že `xa_end` přijímá nestandardní konec 5C6-00D40079.

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

Notes:

- Změna není standardně povolena. Chcete-li použít tuto změnu, musíte zadat klíčové slovo CSQSERVICE1 (v horním případě) kdekoli v poli popisu kanálu SVRCONN používaného klientem XA.
- Kanály s klíčovým slovem CSQSERVICE1 mají následující omezení:
  - Dispozice GROUP odebrání zotavení není povolena. Povolena je pouze dispozice QMGR obnovy zotavení. Dispozice je určena názvem zadaným ve výzvě `xa_open` . Je-li použit název skupiny sdílení front, bude připojení XA vyžadovat skupinovou jednotku zotavení.

    Volání `xa_open` uvádějící název skupiny sdílení front v parametru **`xa_info`** selhává s parametrem *xaer_inval*.
  - Volby *MQGMO_LOCK* a *MQGMO_UNLOCK* nejsou povoleny. Volání MQGET s parametrem *MQGMO_LOCK* nebo *MQGMO_UNLOCK* selže s chybou MQRC_ENVIRONMENT_ERROR.

Související pojmy

“Konfigurace správců transakcí s podporou standardu XA” na stránce 18
Nejprve nakonfigurujte základního klienta produktu IBM MQ a potom nakonfigurujte rozšířenou transakční funkci s použitím informací v těchto tématech.

Formát řetězce xa_open

Řetězec xa_open obsahuje dvojice definovaných názvů parametrů a hodnot.

Řetězec xa_open má následující formát:

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

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

Názvy, významy a platné hodnoty parametrů jsou následující:

Název
Význam a platné hodnoty

CHANNEL
Název kanálu MQI.

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

TRPTYPE
Komunikační protokol pro kanál MQI. Následující protokoly jsou platné hodnoty:

LU62
LU technologie 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 tohoto parametru nejsou citlivé na velikost písmen.

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

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

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

NETBIOS
Název NetBIOS .

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

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

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

TCP
Název hostitele nebo adresa IP, volitelně následované číslem portu v závorkách. Je-li číslo portu vynecháno, předpokládá se výchozí hodnota 1414. Více hostitelů a portů pro správce front lze zadat pomocí oddělovače 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 straně serveru kanálu MQI. Název nesmí být prázdný ani obsahovat jednu hvězdičku (*), ani název nesmí začínat hvězdičkou. To znamená, že tento parametr musí identifikovat konkrétního správce front podle názvu.

Toto je povinný parametr.

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

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

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

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

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

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

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

Jedná se o volitelný parametr.

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

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

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

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

Zde je příklad řetězce xa_open:

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

Parametry CHANNEL, TRPTYPE, CONNAME a QMNAME řetězce xa_open

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

Pokud jsou parametry **CHANNEL** a **CONNAME** zadány v řetězci xa_open, používá rozšířený transakční klient 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 používá hodnotu proměnné prostředí MQSERVER ke spuštění kanálu MQI. Není-li proměnná prostředí MQSERVER definována, bude rozšířený transakční klient používat položku v definici kanálu klienta identifikovanou argumentem **QMNAME** .

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

Pokud se aplikace připojí ke správci front v dřívější verzi než IBM WebSphere MQ 7.0.1, volání xa_open uspěje, ale transakce má dispozici správce front zotavení. z/OS Ujistěte se, že aplikace, které vyžadují dispozice GROUP, se mohou připojovat pouze ke správcům front v produktu IBM WebSphere MQ 7.0.1 nebo novějším.

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

z/OS Pokud se klient aplikace připojuje ke správci front produktu z/OS verze IBM WebSphere MQ 7.0.1 nebo novější, lze pro parametr **QMNAME** zadat název skupiny sdílení front (QSG). To umožňuje

aplikačnímu klientu podílet se na transakci se SKUPINOU transakcí dispozice zotavení. Další informace o jednotce SKUPINY zotavení naleznete v tématu Dispozice jednotky zotavení.

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

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

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

Parametry TPM a AXLIB

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

Je-li parametr TPM zadán v řetězci xa_open, ale parametr AXLIB není zadán, rozšířený transakční klient předpokládá hodnotu parametru AXLIB na základě hodnoty parametru TPM. Viz Tabulka 3 na stránce 23 , kde jsou převzaty hodnoty parametru AXLIB.

Tabulka 3. Předpokládané hodnoty parametru AXLIB

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

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

Další zpracování chyb pro xa_open

Volání xa_open selhává za určitých okolností.

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

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

Zotavení po selhání v rozšířeném transakčního zpracování

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

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

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

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

Struktury přepínačů XA

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

Tyto struktury přepínačů jsou:

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

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

Tyto struktury přepínačů jsou umístěny v knihovnách, které jsou zobrazeny v Tabulka 4 na stránce 24.

Tabulka 4. Knihovny IBM MQ obsahující struktury přepínačů XA

Platforma	**Knihovna obsahující struktury přepínačů XA**
AIX AIX Linux Linux Solaris Solaris	*MQ_INSTALLATION_PATH*/lib/libmqcxa
Systémy Windows Windows	*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 přepínačů.

Související pojmy

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

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

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

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

Použití rozšířeného transakčního klienta s kanály TLS

Není možné nastavit kanál TLS pomocí řetězce xa_open. Postupujte podle těchto pokynů, chcete-li použít tabulku definic kanálů klienta (ccdt).

Informace o této úloze

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

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

Postup

1. Určete řetězec xa_open obsahující pouze povinný parametr qmname (název správce front), například: `XA_Open_String=qmname=MYQM`
2. Pomocí správce front definujte kanál CLNTCONN (client-connection) s požadovanými parametry TLS. Zahrňte název správce front do atributu QMNAME v definici CLNTCONN. Tato hodnota se bude shodovat s názvem qmname v řetězci xa_open.
3. Zpřístupněte definici CLNTCONN pro klientský systém v tabulce definic kanálů klienta (CCDT) nebo v Windowsv aktivním adresáři.
4. Používáte-li tabulku CCDT, identifikujte tabulku CCDT obsahující definici kanálu CLNTCONN s použitím proměnných prostředí MQCHLLIB a MQCHLTAB. Nastavte tyto proměnné v prostředí, které používá aplikace klienta i správce transakcí.

Výsledky

To dává správci transakcí definici kanálu pro příslušného správce front s atributy TLS potřebnými pro ověření správnosti, včetně SSLCIPH, CipherSpec.

Konfigurace rozšířeného transakčního klienta pro produkt CICS

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

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

- Řetězec xa_open
- Úplný název cesty k souboru načtení přepínače

Pro každý z následujících platforem je k dispozici jeden soubor načtení přepínače pro použití produktem CICS :

- AIX
- Solaris
- Windows

Každý soubor pro načtení přepínače obsahuje funkci, která vrací ukazatel na strukturu přepínačů XA, která se používá pro dynamickou registraci, MQRMIXASwitchDynamic. Úplný název cesty pro každý zaváděcí soubor přepínače viz Tabulka 5 na stránce 26 .

Tabulka 5. Soubory načtení přepínače

Platforma	**Zaváděcí soubor přepínače**
AIX Linux Solaris	*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 regionu CICS naleznete v příručce *CICS Administration Reference* a v příručce *CICS Administration Guide* pro vaši platformu.

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

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

  Informace o tom, kdy správce front používá toto ID uživatele pro kontrolu oprávnění, najdete v tématu Zabezpečení.
- Uživatelské procedury ukončení úlohy CICS , které jsou dodávány pro použití v klientských systémech IBM MQ , jsou uvedeny v seznamu Tabulka 6 na stránce 27 . Tyto uživatelské procedury

nakonfigurujete stejným způsobem, jako jste nakonfigurovali odpovídající uživatelské procedury pro systémy serveru IBM MQ . Pro tyto informace se proto podívejte na téma Povolení uživatelských procedur CICS.

Tabulka 6. Ukončení ukončení úlohy CICS

Platforma	Zdroj	Knihovna
AIX AIX Linux Linux Solaris Solaris	amqzscgx.c	amqczscg
Systémy Windows Windows	amqzscgn.c	mqcc1415.dll

Konfigurace rozšířeného transakčního klienta pro Tuxedo

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

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

- V sekci GROUPS v souboru UBBCONFIG produktu Tuxedo pro aplikaci použijte parametr **OPENINFO** k určení řetězce xa_open. Příklad toho, jak to provést, najdete v ukázkovém souboru UBBCONFIG, který je dodáván pro použití s ukázkovými programy produktu Tuxedo.

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

  - AIX
  - Solaris

  Windows Windows, název souboru je `ubbstxcn.cfg`.

- V položce pro správce front v tabulce správce prostředků produktu Tuxedo zadejte název struktury přepínače XA a úplný název cesty knihovny, která obsahuje strukturu:

  - UNIX V systémech AIX a Solariszadejte `udataobj/RM`.
  - Windows V systému Windowszadejte `udataobj\rm`.

  Příklad toho, jak to lze provést pro jednotlivé platformy, najdete v tématu Ukázky TUXEDO.
  Produkt Tuxedo podporuje dynamickou registraci správce prostředků, a proto můžete použít buď MQRMIXASwitch, nebo MQRMIXASwitchDynamic.

Windows Microsoft Transakční server

Před použitím správce transakcí produktu Microsoft Transaction Server (MTS) jako správce transakcí není nutná žádná další konfigurace. Existují však body, které je třeba poznamenat.

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

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

  Když se aplikace MTS připojí ke správci front serveru a spustí kanál MQI, rozšířený transakční klient extrahuje dostatečné informace z parametrů volání MQCONN nebo MQCONNX, aby umožnil opětovné

spuštění kanálu po selhání, pokud je to požadováno. Rozšířený transakční klient předává informace do MTS a MTS zaznamenává informace do svého protokolu.

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

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

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

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

- Všimněte si následujících podmínek, když používáte rozšířeného transakčního klienta s MTS:
  - V rámci jednoho podprocesu může být klientská aplikace připojena pouze k jednomu správci front v daném okamžiku.
  - Každý podproces aplikace klienta se může připojit k jinému správci front.
  - Klientská aplikace nemůže používat sdílené obslužné rutiny připojení.

Definování kanálů MQI

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

Kanály definované uživatelem

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

Tyto dvě metody jsou podrobně popsány:

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

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

   Podrobné informace o způsobu použití této metody naleznete v příručce “Vytváření připojení k serveru a připojení klienta na různých platformách” na stránce 34 .
2. Vytvořte obě definice kanálů na počítači serveru.

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

   Podrobné informace o způsobu použití této metody naleznete v příručce “Vytvoření připojení k serveru a připojení klienta na serveru” na stránce 39 .

Automaticky definované kanály

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

Je-li požadavek na připojení typu Inbound obdržen od klienta a nelze v daném správci front nalézt odpovídající definici připojení k serveru, produkt IBM MQ ji automaticky vytvoří a přidá do správce front. Automatická definice je založena na definici výchozího kanálu připojení serveru SYSTEM.AUTO.SVRCONN. Automatickou definici definic připojení serveru můžete povolit aktualizací objektu správce front pomocí příkazu ALTER QMGR s parametrem CHAD (nebo pomocí příkazu PCF Change Queue Manager s parametrem ChannelAutoDef).

Související pojmy

"Řídicí funkce kanálu" na stránce 199

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

ULW Vytvoření a použití kanálů AMQP

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

Než začnete

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

- AIX Komponenty produktuIBM MQ pro systémy AIX
- Linux Komponenty IBM MQ rpm pro systémy Linux
- Linux KomponentyIBM MQ Debian pro systémy Linux Ubuntu
- Solaris Komponenty produktuIBM MQ pro systémy Solaris
- Windows Funkce produktuIBM MQ pro systémy Windows

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

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

Informace o této úloze

Následující procedura předpokládá, že máte existujícího správce front.

Pokud vyžadujete nového správce front, je zahrnut ukázkový skript, který je umístěn v adresáři *mqinstall*/amqp/samples . Skript vytvoří nového správce front, spustí službu AMQP, vytvoří nový kanál s názvem SAMPLE.AMQP.CHANNELa spustí kanál.

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

Windows Linux Pokud spustíte vzorový skript, buď SampleMQM.sh na Linux, nebo SampleMQM.bat na Windows, můžete spustit následující proceduru na "6" na stránce 30.

Můžete použít výchozí kanál SYSTEM.DEF.AMQP, otestujte připojení produktu MQ Light ke správci front nebo můžete vytvořit nový kanál.

Následující procedura používá výchozí kanál.

Postup

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

   ```
   runmqsc QMNAME
   ```

2. V 9.1.0
   (Nezbytné pouze v případě, že je správce front IBM MQ 9.0.4 nebo dřívější.) Zkontrolujte, zda je funkce AMQP nainstalována a funguje správně.

Ke spuštění služby IBM MQ , která ovládá prostředí JVM, použijte příkaz **START SERVICE** :

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

Poznámka: V systému IBM MQ 9.1 je SYSTEM.AMQP.SERVICE má nastaven atribut **CONTROL** na hodnotu *QMGR*. To způsobí, že bude služba spuštěna automaticky, když je spuštěn správce front. Nastavením atributu **CONTROL** na hodnotu *MANUAL*můžete zabránit spuštění služby při spuštění správce front.

Po spuštění správce front budou automaticky spuštěny služby AMQP a kanál AMQP, jsou-li definovány.

3. Nastavte ID uživatele MCAUSER .

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

   Poznámka: Windows V Windows, před IBM MQ 9.1.1, je nastavení ID uživatele MCAUSER podporováno pouze pro ID uživatelů o délce až 12 znaků.

   V 9.1.1 Od verze IBM MQ 9.1.1 již neplatí limit délky max. 12 znaků.

   a) Použijte příkaz **ALTER CHANNEL** k nastavení ID uživatele MCAUSER :

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

   b) Pomocí následujících dvou příkazů **setmqaut** můžete autorizovat své ID uživatele MCAUSER pro publikování a přihlášení k odběru témat:

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

   a

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

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

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

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

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

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

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

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

6. Změňte výchozí port.

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

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

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

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

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

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

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

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

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

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

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

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

   - V 9.1.5 V 9.1.0.5 Pokud nastavíte atribut **SSLCAUTH** na hodnotu REQUIRED, bude možné zkontrolovat rozlišující název (DN) certifikátu od klienta. Chcete-li zkontrolovat rozlišující název certifikátu od klienta, nastavte atribut **SSLPEER** . Chcete-li zkontrolovat rozlišující název certifikátu od klienta, použijte příkaz **ALTER CHANNEL** . Příklad:

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

     Případně můžete také použít záznamy ověření kanálu k povolení nebo blokování připojení, protože tato metoda nabízí větší granularitu ve srovnání s použitím atributu **SSLPEER** . Další informace o nastavení **SSLPEER** a použití záznamů ověření kanálu jako alternativy najdete v tématu SSL Peer.
9. Nainstalujte klienta MQ Light Node.js spuštěním následujícího příkazu:

```
npm install mqlight
```

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

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

      ```
      node recv.js
      ```

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

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

Při úspěšném připojení k výchozímu kanálu se zobrazí následující zpráva:

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

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

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

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

```
node send.js
```

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

12. Ukázka **AMQSSUB** IBM MQ se používá k přijetí ukázkové zprávy produktu MQ Light .

V systémech Linux a Windowslze ukázku nalézt v následujících umístěních:

- Linux *mqinstall*`/samp/bin` v systému Linux.
- Windows *mqinstall*`/Tools\c\Samples\Bin` v systému 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. Chcete-li vytvořit více kanálů AMQP, použijte příkaz **DEFINE CHANNEL** :

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

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

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

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

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

Jak pokračovat dále

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

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

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

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

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

Poznámka: Neodstraňujte výchozí kanál SYSTEM.DEF.AMQP.

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

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

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

ULW 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 produktu IBM MQ pro rozhraní API produktu MQ Light :
   - AIX V produktu AIX spusťte následující příkaz:

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

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

     ```
     rpm -e MQSeriesAMQP
     ```

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

Související úlohy
Vyvíjení klientských aplikací AMQP
Zabezpečení klientů AMQP

ULW Soubory protokolu kanálu AMQP

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

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

Výchozí datový adresář na Linux je /var/mqm.

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

- amqp.stdout, zapsána do složky qmgrs/*QM-name* .

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

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

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

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

Související pojmy

Chybové protokoly v systému UNIX, Linux, and Windows

Související úlohy

Vyvíjení klientských aplikací AMQP

Zabezpečení klientů AMQP

Vytváření připojení k serveru a připojení klienta na různých platformách

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

Informace o této úloze

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

z/OS V systému z/OS můžete také použít panely Operace a Ovládací panely.

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

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

Následující pokyny se týkají, když produkt **runmqsc**:

- Můžete zadat parametr **-c** a volitelně parametr **-u** pro připojení **runmqsc** jako klienta ke správci front, kterého chcete spravovat.
- Použijete-li parametr **-u** k zadání ID uživatele, budete vyzváni k zadání odpovídajícího hesla.
- Pokud jste záznam `CONNAUTH AUTHINFO` nakonfigurovali s `CHCKLOCL(REQUIRED)` nebo `CHCKLOCL(REQDADM)`, musíte použít parametr **-u** , jinak nebudete schopni spravovat správce front s **runmqsc**.

Procedura

- Chcete-li na serveru definovat kanál připojení serveru, prohlédněte si téma “Definování kanálu připojení serveru na serveru” na stránce 34.
- Chcete-li vytvořit kanál připojení klienta na systému IBM MQ MQI client, přejděte na téma “Vytvoření kanálu připojení klienta v systému IBM MQ MQI client pomocí MQSERVER” na stránce 35.

Definování kanálu připojení serveru na serveru

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

Postup

1. Volitelné: Pokud vaše platforma serveru není z/OS, nejprve vytvořte a spusťte správce front a poté spusťte příkazy MQSC.

a) Vytvořte správce front s názvem QM1 , například:

```
crtmqm QM1
```

b) Spusťte správce front:

```
strmqm QM1
```

c) Spusťte příkazy MQSC:

```
runmqsc QM1
```

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

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

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

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

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

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

Můžete zvolit identifikaci vašeho příchozího připojení pomocí několika různých atributů. Příklad používá adresu IP. Alternativní atributy zahrnují ID uživatele klienta a rozlišující název TLS Subject Distinguished Name. Další informace naleznete v tématu Záznamy ověřování 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 UNIX V systému UNIX 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 UNIX V systému UNIX 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 UNIX V systému UNIX 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.

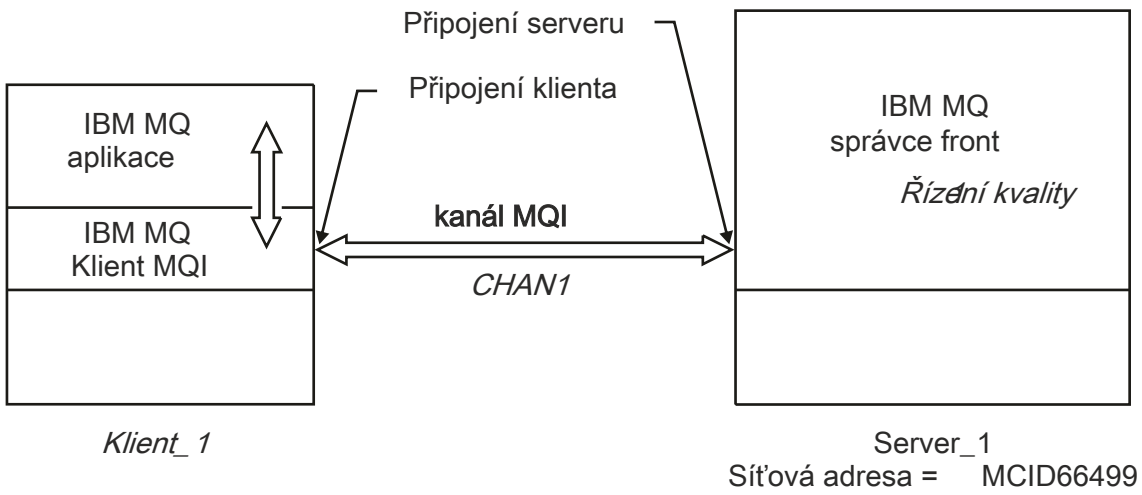
- Chcete-li zrušit soubor **MQSERVER** a vrátit se do tabulky definic kanálů klienta, na kterou ukazují **MQCHLLIB** a **MQCHLTAB**, zadejte následující příkaz:
  - Linux UNIX V systému UNIX and Linux:

    ```
    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 UNIX V systému UNIX 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 “Předvolený port 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 UNIX V systému UNIX and Linux:

```
export MQSERVER=CHANNEL1/TCP/'9.20.4.56'
export MQSERVER=CHANNEL1/LU62/B0X99
```

  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 60
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.

Předvolený port TCP/IP

Při výchozím nastavení pro protokol TCP/IP produkt IBM MQ předpokládá, že kanál bude připojen k portu 1414.

Tento stav můžete změnit takto:

- Přidání čísla portu v hranatých závorkách jako poslední části pole ConnectionName:
  - Windows V systému Windows:

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

  - Linux UNIX V systému UNIX and Linux:

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

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

```
TCP:
port=2001
```

- Přidejte IBM MQ do souboru služeb, jak je popsáno v tématu “Použití modulu listener protokolu TCP/IP v systému UNIX and Linux” na stránce 239.

Výchozí soket SPX

Při výchozím nastavení pro protokol SPX předpokládá produkt IBM MQ , že kanál bude připojen k soketu 5E86.

Tento stav můžete změnit takto:

- Přidání čísla soketu do hranatých závorek jako poslední části pole ConnectionName:

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

U připojení SPX zadejte hodnotu ConnectionName a soket ve formě `network.node(socket)`. Pokud se klient a server IBM MQ nacházejí ve stejné síti, nemusí být tato síť zadána. Pokud používáte výchozí soket, nemusí být určen soket.

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

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

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 35
Kanál připojení klienta na pracovní stanici klienta můžete definovat pomocí proměnné prostředí **MQSERVER** .

Vytvoření připojení k serveru a připojení klienta na serveru

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

Informace o této úloze

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

- Na všech platformách můžete pomocí příkazů skriptu IBM MQ Script (MQSC), pomocí příkazů programu PCF (Programmable command Format) definovat kanál připojení serveru na počítači serveru.
- Windows Linux V systémech Linux a Windowsmůžete rovněž použít produkt IBM MQ Explorer.
- z/OS V systému z/OSmůžete také použít panely Operace a Ovládací panely.
- IBM i V systému IBM i můžete také použít rozhraní panelu.

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

Postup

1. Chcete-li definovat kanál připojení serveru, přečtěte si téma “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 53.

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 53
Po definování kanálu připojení serveru nyní definujete odpovídající kanál připojení klienta.

“Přístup k definicím kanálu připojení klienta” na stránce 54
Můžete vytvořit tabulku CCDT (Client Channel Definition CCDT) pro klientské aplikace tak, že ji zkopírujete nebo ji budete sdílet, poté zadejte jeho umístění a název na klientském počítači. V produktu IBM MQ 9.0poskytuje produkt IBM MQ také schopnost vyhledat tabulku definic kanálů klienta (CCDT) prostřednictvím adresy URL.

Konfigurace tabulek definic kanálů klienta

Tabulka definic kanálů klienta (CCDT) definuje kanály připojení klienta a jejich atributy. Klienti čtou tento soubor, aby určili, ke kterým správcům front se má připojit. Soubor CCDT může být buď formát JSON, nebo binární formát.

Informace o této úloze

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

V 9.1.2 Před IBM MQ 9.1.2je tabulka CCDT dostupná pouze v binárním formátu. V produktu IBM MQ 9.1.2můžete také vytvořit tabulku CCDT ve formátu JavaScript Object Notation (JSON).

Soubor CCDT s binárním formátem je vytvořen automaticky při vytvoření správce front. Aktualivujte definice kanálů klienta uložené v této tabulce pouze s použitím příkazu **runmqsc** .

V 9.1.2 Formát JSON tabulky CCDT je prostý textový soubor s příponou .json. Tuto tabulku můžete vytvořit a aktualizovat ručně, což je méně omezující než použití příkazu **runmqsc** .

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

Chcete-li vám pomoci s konfigurací CCDT pro práci s klienty, vyberte si z následujících úloh:

Procedura

- “Konfigurace binárního formátu CCDT” na stránce 41
- V 9.1.2

“Konfigurace formátu JSON CCDT” na stránce 43
- “Umístění pro tabulky CCDT” na stránce 50
- “Přístup URL k tabulce CCDT” na stránce 51

Související pojmy
Jednotné klastry
Klient MQI: Tabulka definic kanálů klienta (CCDT)

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

V 9.1.2 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 43.

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 UNIX Na systémech UNIX and Linux:

/prefix/qmgrs/*QUEUEMANAGERNAME*/@ipcc

Název adresáře, na který odkazuje *QUEUEMANAGERNAME* , rozlišuje velká a malá písmena na systémech UNIX 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 50.

  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 adresy URL, definováním 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 50 .

- 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) V tabulce CCDT nastavte atribut správce front **SSLCRLNL** na název seznamu názvů.

Související pojmy

Práce se zrušenými certifikáty

Související úlohy

“Konfigurace formátu JSON CCDT” na stránce 43

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.

V 9.1.2 *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**
ULW UNIX platformy, Linuxa 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 47 a “Atributy kanálu podporované CCDT JSON” na stránce 45.
- 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 50.
- 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:

  - UNIX Na systémech UNIX:

    `$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 adresy URL, definováním 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 50 .
- 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

Jednotné klastry

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.

V 9.1.2 *Atributy kanálu podporované CCDT JSON*

Seznam atributů kanálu připojení klienta podporovaných službou CCDT JSON. Tento seznam je podmnožinou atributů podporovaných binární tabulky 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 případy použití najdete v tématu “Příklady JSON CCDT” na stránce 47 .

Úplný seznam dostupných atributů a jejich možných hodnot najdete v tématu Atributy kanálu v abecedním pořadí.

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

Upozornění: Požadované atributy jsou kanál **name** a kanál **type**. Pokud také definujete **portRange**, jsou vyžadovány také atributy *low* a *high* .

Objekt JSON	Klíč JSON	datový typ JSON	Definice binárního atributu
kanál (pole)	název	String	CHANNEL

Objekt JSON	Klíč JSON	datový typ JSON	Definice binárního atributu
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
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	změněné	String	ALTDATE a ALTTIME
channel.transmissionSecurity	certificateLabel	String	CERTLABL
channel.transmissionSecurity	Název certificatePeer	String	SSLPEER
channel.transmissionSecurity	cipherSpecification	String	SSLCIPH

Notes:

- `channel.connectionManagement.localAddress` může být definován jako jedna z následujících kombinací kláves:
  - Hostitel a port
  - hostitel a portRange
  - Port
  - portRange
- Klíč `channel.timestamps altered` JSON je volitelný a, pokud není definován, hodnota standardně zobrazuje čas poslední změny souboru JSON tabulky CCDT. Je-li však prostředí nakonfigurováno pro načtení tabulky CCDT z adresy URL, výchozí hodnota je čas posledního stažení souboru.
- `channel.clientConnection.connection` musí zahrnovat jak hostitele, tak klíče portu.
- Pozměněný klíč je jediný řetězec, který zapouzdřuje atributy parametru ALTDATE i ALTTIME.
- Typ transportu může být pouze TCP, proto nejsou ve schématu definovány následující atributy:
  - **TRPTYPE**
  - **USERID**
  - **PASSWORD**
  - **MODENAME**
  - **TPNAME**

Související odkazy
Atributy kanálu pro typy kanálů

V 9.1.2 *Příklady JSON CCDT*
Použijte příklady uvedené v tomto tématu jako základ pro vaše požadavky.

Otevřete generický textový editor a zkopírujte jeden z následujících příkladů:

- “Definujte jednoduché připojení klienta” na stránce 47
- “Definování jednoho kanálu a jednoho správce front pomocí protokolu TLS” na stránce 48
- “Definujte jeden kanál a jeden správce front, který nepoužívá TLS” na stránce 48
- “Definovat dva kanály se stejným názvem” na stránce 48
- “Úplný seznam definic atributů kanálu CCDT” na stránce 49

Definujte jednoduché připojení klienta

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

Definování jednoho kanálu 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"
    }
  ]
}
```

Definujte jeden kanál a jeden správce front, který nepoužívá 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 různým 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

```
{
  "channel":
  [
    {
      "compression":
      {
        "header": [ "system" ],
        "message": [ "zlibfast" ]
      },
      "connectionManagement":
      {
        "sharingConversations": 10,
        "clientWeight": 1,
        "affinity": "none",
        "defaultReconnect": "yes",
        "disconnectInterval": 6000,
        "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, adresy URL protokolu FTP nebo HTTP. 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.

Z produktu IBM MQ 9.0může být tabulka CCDT hostována v centrálním umístění, které je přístupné prostřednictvím adresy URL, což odstraňuje potřebu individuální aktualizace tabulky CCDT pro každého implementovaného klienta. Produkt IBM MQ 9.0 přidal funkci pro nativní (C/C + +, COBOL a RPG) a nespravované aplikace .NET pro stažení tabulky CCDT z adresy URL, ať už se jedná o lokální soubor, FTP nebo prostředek 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 adresy 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 protokolem 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 jednotlivých klientech. Další informace viz téma “Přístup URL k tabulce CCDT” na stránce 51.

Jak určit umístění tabulky CCDT na klientovi

V klientském systému můžete určit umístění tabulky CCDT následujícími způsoby:

- Pomocí proměnných prostředí `MQCHLLIB` určete adresář, ve kterém je tabulka umístěna, a pomocí proměnné prostředí `MQCHLTAB` zadejte název souboru tabulky.
- Použití konfiguračního souboru klienta. V sekci `CHANNELS` použijte atributy `ChannelDefinitionDirectory` k uvedení adresáře, kde je tabulka umístěna, a `ChannelDefinitionFile` k uvedení názvu souboru.
- Poskytnutím adresy 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 použijete adresu 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 51.

Přístup URL k tabulce CCDT

Můžete hostovat tabulku CCDT (Client Channel Definition Table) v centrálním umístění, ke kterému lze přistupovat prostřednictvím adresy URL, a odstranit tak potřebu individuální aktualizace tabulky CCDT pro každého implementovaného klienta.

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

- Programováním pomocí MQCNO
- Pomocí proměnných prostředí

  Upozornění: Volbu proměnné prostředí můžete použít pouze pro nativní programy, které se připojují jako klienti, tj. aplikace v jazycích 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, adresy URL protokolu FTP nebo http.
- Pomocí sekce CHANNELS souboru `mqclient.ini` .

Proměnná prostředí **MQCCDTURL** vám umožňuje poskytnout soubor, adresu URL protokolu FTP nebo adresu URL protokolu HTTP 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 CHANNELS konfiguračního souboru klienta” na stránce 155) k vyhledání souboru CCDT, buď prostřednictvím souboru, ftp, nebo adresy URL http, 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 adresy URL.

Základní ověření u připojení je podporováno prostřednictvím pověření zakódovaných v adrese 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 adrese URL.

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

1. MQCD poskytovaný produktem **ClientConnOffset** a **ClientConnPtr** v MQCNO.
2. Adresa URL poskytnutá **CCDTUrlOffset** a **CCDTUrlPtr** v MQCNO.
3. Proměnná prostředí MQSERVER .
4. Pokud je definován soubor `mqclient.ini` a obsahuje parametry ServerConnection, použije se kanál, který definuje. Další informace naleznete v tématu “IBM MQ MQI client konfigurační soubor mqclient.ini” na stránce 143 a “Sekce CHANNELS konfiguračního souboru klienta” na stránce 155.
5. **MQCCDTURL** proměnná prostředí.
6. **MQCHLLIB** a **MQCHLTAB** proměnná prostředí.
7. **ChannelDefinitionDirectory** a **ChannelDefinitionFile** v souboru “Sekce CHANNELS konfiguračního souboru klienta” na stránce 155.

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

Při pokusu o otevření souboru CCDT pro přístup pro zápis, například při použití příkazu **runmqsc** DEFINE CHANNEL z klienta, se zobrazí chybová zpráva informující o tom, že soubor nelze otevřít pro přístup pro zápis.

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

Související úlohy

“Přístup k definicím kanálu připojení klienta” na stránce 54
Můžete vytvořit tabulku CCDT (Client Channel Definition CCDT) pro klientské aplikace tak, že ji zkopírujete nebo ji budete sdílet, poté zadejte jeho umístění a název na klientském počítači. V produktu IBM MQ 9.0poskytuje produkt IBM MQ také schopnost vyhledat tabulku definic kanálů klienta (CCDT) prostřednictvím adresy 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 Active Directory

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

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

1. Datová struktura MQCONNX MQCD
2. proměnná prostředí MQSERVER
3. definiční soubor kanálu klienta
4. Active Directory

Toto pořadí znamená, že žádné aktuální aplikace nebudou ovlivněny žádnou změnou. Tyto záznamy v Active Directory si můžete představit jako záznamy v souboru definic kanálů klienta a klient IBM MQ

je zpracovává stejným způsobem. Chcete-li nakonfigurovat a spravovat podporu pro publikování definic kanálů připojení klienta v Active Directory, použijte příkaz `settqscp` , jak je popsáno v souboru 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')
```

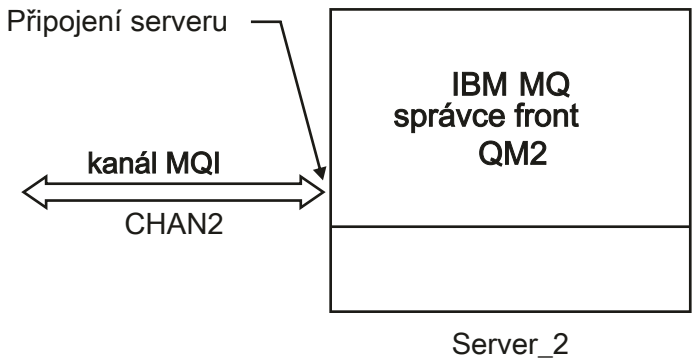
2. Chcete-li povolit přístup pro příchozí připojení ke správci front, použijte následující příkaz:

```
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

Definování kanálu připojení klienta na serveru

Po definování kanálu připojení serveru nyní definujete odpovídající kanál připojení klienta.

Než začnete

Definujte kanál připojení serveru.

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:

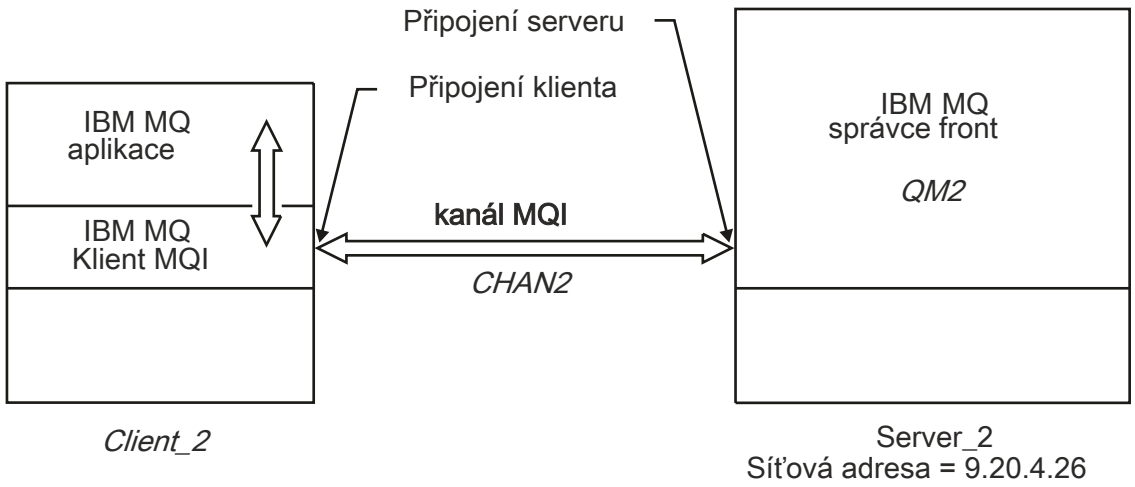
```
SET CHLAUTH(CHAN2) TYPE(ADDRESSMAP) ADDRESS('IP-address') MCAUSER('userid')
```

   - Kde 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

Přístup k definicím kanálu připojení klienta

Můžete vytvořit tabulku CCDT (Client Channel Definition CCDT) pro klientské aplikace tak, že ji zkopírujete nebo ji budete sdílet, poté zadejte jeho umístění a název na klientském počítači. V produktu IBM MQ 9.0poskytuje produkt IBM MQ také schopnost vyhledat tabulku definic kanálů klienta (CCDT) prostřednictvím adresy URL.

Než začnete

Tato úloha předpokládá, že jste definovali v tabulce CCDT klientské kanály připojení, které potřebujete. Viz “Konfigurace tabulek definic kanálů klienta” na stránce 40.

Informace o této úloze

Má-li klientská aplikace používat tabulku CCDT (Client Channel Definition CCDT), je třeba k ní zpřístupnit tabulky CCDT a zadat její umístění a název. Existuje několik způsobů, jak to provést:

- CCDT můžete zkopírovat na klientský počítač.
- CCDT můžete zkopírovat do umístění sdíleného více než jedním klientem.
- Nástroje CCDT lze zpřístupnit klientovi jako sdílený soubor, zatímco zůstává umístěn na serveru.

Z produktů IBM MQ 9.0, IBM MQ, nativních (C/C + +, COBOL a RPG) a nespravovaných aplikací .NET mohou tabulky CCDT hostované v centrálním umístění z adresy URL, ať už se jedná o lokální soubor, ftp nebo prostředek http.

Postup

1. Zpřístupněte tabulky CCDT klientským aplikacím jedním z následujících způsobů:
   a) Volitelné: Zkopírujte tabulky CCDT na klientský počítač.
   b) Volitelné: Zkopírujte tabulku CCDT do umístění sdíleného více než jedním klientem.
   c) Volitelné: Opustit CCDT na serveru, ale umožnit jeho sdílení klientem.
   d) Volitelné: Definujte lokální soubor, protokol FTP nebo adresu URL http pro tabulku CCDT hostované v centrálním umístění, aby nativní (C/C + +, COBOL a RPG) a nespravované aplikace .NET mohly tabulku CCDT stáhnout z této adresy URL.

   Bez ohledu na umístění, které jste vybrali pro tabulky CCDT, musí být umístění zabezpečeno, aby se zabránilo neautorizovaným změnám kanálů.
2. Na straně klienta zadejte umístění a název souboru obsahujícího tabulky CCDT jedním ze tří způsobů:
   a) Volitelné: Použijte sekci CHANNELS konfiguračního souboru klienta. Další informace viz téma “Sekce CHANNELS konfiguračního souboru klienta” na stránce 155.
   b) Volitelné: Použijte proměnné prostředí MQCHLLIB a MQCHLTAB.

      Proměnné prostředí můžete nastavit například zadáním příkazu:

      - V systémech UNIX and Linux :

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

      - IBM i V systému 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 v Active Directory.
   d) Poskytněte umístění centrálně hostované tabulky CCDT prostřednictvím adresy URL, buď programováním pomocí proměnné prostředí MQCNO, pomocí proměnných prostředí, nebo pomocí oddílů souboru `mqclient.ini` . Další informace viz “Umístění pro tabulky CCDT” na stránce 50 a “Přístup URL k tabulce CCDT” na stránce 51.

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

Související pojmy

“Přístup URL k tabulce CCDT” na stránce 51

Můžete hostovat tabulku CCDT (Client Channel Definition Table) v centrálním umístění, ke kterému lze přistupovat prostřednictvím adresy URL, a odstranit tak potřebu individuální aktualizace tabulky CCDT pro každého implementovaného klienta.

Klient MQI: Tabulka definic kanálů klienta (CCDT)

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.

ULW Programy pro ukončení kanálů pro kanály MQI

Tři typy ukončení kanálu jsou k dispozici pro prostředí produktu IBM MQ MQI client v systému UNIX, Linux, and Windows.

Patří mezi ně:

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

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

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

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

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

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

Související pojmy

“Zabezpečení se ukončí na připojení klienta” na stránce 57
Ukončovací programy zabezpečení můžete použít k ověření, že partner na druhém konci kanálu je pravý. Speciální pokyny platí, je-li pro připojení klienta použita uživatelská procedura pro zabezpečení zprávy.

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

Související úlohy

Rozšíření zařízení 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 rozhraní API v ukončovacím programu pro odeslání nebo přijetí” na stránce 58

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

ULW 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 UNIX, Linux, and Windows je do vašeho systému přidán konfigurační soubor klienta během instalace IBM MQ MQI client. Předvolená cesta pro umístění kanálů kanálu na klientovi je definovaná v tomto souboru, za použití stanzy:

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

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

Při inicializaci kanálu po volání funkce MQCONN nebo volání MQCONNX je prohledáván konfigurační soubor klienta. Stanza ClientExitje přečtena a všechny uživatelské procedury kanálu, které jsou určeny v definici kanálu, jsou načteny.

ULW Zabezpečení se ukončí na připojení klienta

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

Obrázek 4 na stránce 58 ilustruje použití uživatelských procedur zabezpečení v připojení klienta pomocí správce oprávnění objektu IBM MQ k ověření uživatele. Ve struktuře MQCNO na straně klienta je ve struktuře MQCNO nastavena hodnota SecurityParmsPtr nebo SecurityParmsOffset a existují uživatelské procedury zabezpečení na obou koncích kanálu. Po dokončení běžné výměny zpráv zabezpečení a ke spuštění kanálu je struktura MQCSP přístupná z pole MQCXP SecurityParms předána do uživatelské procedury zabezpečení na straně klienta. Typ ukončení je nastaven na hodnotu MQXR_SEC_PARMS. Uživatelská procedura zabezpečení se může rozhodnout neprovádět nic pro identifikátor uživatele a heslo, nebo může změnit jednu nebo obě z nich. Data vrácená z uživatelské procedury se pak odešlou na konec kanálu na připojení serveru. Struktura MQCSP je znovu sestavena na konci kanálu připojení k serveru a je předána uživatelské proceduře zabezpečení připojení k serveru z pole MQCXP SecurityParms . Uživatelská procedura zabezpečení přijímá a zpracovává tato data. Toto zpracování obvykle provádí obrácení změn provedených v polích ID uživatele a hesla v uživatelské proceduře klienta, které se pak používají k autorizaci připojení ke správci front. Výsledná struktura MQCSP se odkazuje pomocí parametru SecurityParmsPtr ve struktuře MQCNO v systému správce front.

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

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

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

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

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

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

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

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

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

Poznámka: Aplikace uživatelské procedury zabezpečení postavené před vydáním produktu IBM WebSphere MQ 7.1 mohou vyžadovat aktualizaci. Další informace najdete v tématu Uživatelské programy zabezpečení kanálu.

ULW Identifikace volání rozhraní API v ukončovacím programu pro odeslání nebo přijetí

Při použití kanálů MQI pro klienty určuje bajt 10 vyrovnávací paměti volání rozhraní API, které má být používáno při volání uživatelské procedury pro odesílání nebo příjem. To je užitečné k identifikaci toho,

které toky kanálu obsahují uživatelská data a mohou vyžadovat zpracování, jako je šifrování nebo digitální podepisování.

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

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

Tabulka 8. Identifikace volání rozhraní API

Volání rozhraní API	**Hodnota bajtu 10 pro požadavek**	**Hodnota bajtu 10 pro odpověď**
MQCONN “1” na stránce 59, “2” na stránce 59	X'81 '.	X "91"
MQDISC “1” na stránce 59	X'82 '	X "92"
MQOPEN “3” na stránce 59	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"
Požadavek 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_	X'A5'	X'B5'
Požadavek xa_commit	X'A6'	X'B6'
Požadavek xa_rollback	X'A7'	X'B7'
požadavek-xa_	X'A8'	X'B8'
Požadavek xa_rec	X'A9'	X'B9'
požadavek xa_complete	X'AA '	X'BA '

Notes:

1. Připojení mezi klientem a serverem je zahájeno klientskou aplikací pomocí MQCONN. Proto je pro tento příkaz zejména několik dalších toků sítě. To samé platí pro MQDISC, které ukončuje síťové připojení.
2. MQCONNX je pro účely připojení typu klient-server zpracován stejným způsobem jako MQCONN.
3. Je-li otevřen rozsáhlý distribuční seznam, může existovat více než jeden tok sítě na volání MQOPEN, aby byla předána všechna požadovaná data do kanálu SVRCONN MCA.

4. Velké zprávy mohou překročit velikost segmentu přenosu. Pokud k tomu dojde, může existovat mnoho síťových toků, které jsou výsledkem jediného volání rozhraní API.

z/OS Připojení klienta ke skupině sdílení front

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

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

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

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

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

Postup

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

1. Definujte kanál SVRCONN, jak je uvedeno v následujícím příkladu:

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

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

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

Výsledky

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

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. Tyto příkazy jsou k dispozici na všech platformách IBM MQ MQI client , není-li uvedeno jinak. Formát příkazu závisí na vaší platformě. Příklad:

- Linux UNIX V systému UNIX 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)
```

Kde je to možné, produkt IBM MQ použije výchozí hodnoty pro proměnné, 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 UNIX
  V systému UNIX 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

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 81
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 UNIX V systémech UNIX 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

V 9.1.1 Multi

V produktu IBM MQ 9.1.1můžete 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 se však negeneruje, 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

V 9.1.0.2 V 9.1.2 Multi

V systémech IBM MQ 9.1.0 Fix Pack 2 a IBM MQ 9.1.2můžete pomocí proměnné prostředí **AMQ_CONVEBCDICNEWLINE** určit, jak má IBM MQ převést znak NL EBCDIC na formát ASCII. Proměnná prostředí má stejné hodnoty jako atribut **ConvEBCDICNewline** `mqs.ini`, tj. `NL_TO_LF`, `TABLE`nebo `ISO` (viz "AllQueueSekce správců souboru mqs.ini" na stránce 87). 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

V 9.1.0

Pokud je v systému IBM MQ 9.1proměnná 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, 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

V 9.1.5 V 9.1.0.5

V systémech IBM MQ 9.1.0 Fix Pack 5 a IBM MQ 9.1.5dotazy na dispozice správce front, které jsou standardně používány příkazem **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).

METRIC_LICENCOVÁNÍ_AMQ_METRIKY

Nastavení proměnné prostředí **AMQ_LICENSING_METRIC=VPCMonthlyPeak** v produktu IBM MQ 9.1.1způsobí, že správce front odešle data související s měsíčními typy licencí VPC namísto výchozího chování při odesílání dat souvisejících s hodinovými licencemi založenými na kontejnerech.

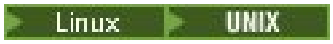
Další informace o konfiguraci produktu IBM MQ pro použití se službou měření IBM Cloud Private naleznete v části IBM Cloud Private služba měření v dokumentaci k produktu IBM Cloud Private .

AMQ_LDAP_TRACE

V systémech IBM MQ 9.1.0 Fix Pack 4 a IBM MQ 9.1.4platí, že 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.

AMQ_MQS_INI_LOCATION



Na systémech UNIX 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, viz “IBM MQ konfigurační soubor mqs.ini” na stránce 82.

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 jinéhonežIBM 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.

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

V systémech IBM MQ 9.0.0 Fix Pack 1 a IBM MQ 9.0.2platí, že není-li nastavena proměnná prostředí **AMQ_SSL_ALLOW_DEFAULT_CERT** , 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 “Sekce SSL konfiguračního souboru klienta” na stránce 164.

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.

GMQ_MQ_LIB

Jsou-li v systému nainstalovány servery IBM MQ MQI client i IBM MQ , standardně se na serveru spouštějí třídy automatizace IBM MQ pro aplikace ActiveX (MQAX). Chcete-li spustit MQAX pro klienta, musí být v proměnné prostředí **GMQ_MQ_LIB** určena knihovna vazeb klienta, například nastavit `GMQ_MQ_LIB=mqic.dll`. V případě instalace pouze klienta není nutné nastavovat proměnnou prostředí **GMQ_MQ_LIB** . Není-li tato proměnná prostředí nastavena, IBM MQ se pokusí načíst `amqzst.dll`. Pokud tato knihovna DLL není přítomna (jak je tomu v případě instalace pouze klienta), IBM MQ se pokusí načíst `mqic.dll`.

HOME

V systémech UNIX, 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 naleznete v tématech “IBM MQ MQI client konfigurační soubor mqclient.ini” na stránce 143 a “Umístění konfiguračního souboru klienta” na stránce 145.

HOMEDRIVE a HOMEPATH

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 naleznete v tématech “IBM MQ MQI client konfigurační soubor mqclient.ini” na stránce 143 a “Umístění konfiguračního souboru klienta” na stránce 145.

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 SuppressInterval v souboru “Konfigurační soubory správce front qm.ini” na stránce 95 .

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 “Konfigurační soubory správce front qm.ini” na stránce 95 , kromě toho, 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

ULW V 9.1.3

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” na stránce 10.

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** určuje adresář pro výstup protokolu a trasování pro IBM MQ classes for JMS a IBM MQ classes for Java. Používá se ve skriptech dodávaných s IBM MQ classes for JMS a IBM MQ classes for Java.

Další informace naleznete v tématu Nastavení proměnných prostředí pro třídy IBM MQ pro platformu JMS a Proměnné prostředí související s třídami IBM MQ pro jazyk Java.

MQ_JAVA_INSTALL_PATH

Proměnná prostředí **MQ_JAVA_INSTALL_PATH** určuje adresář, ve kterém je nainstalován produkt IBM MQ classes for JMS , jak je uvedeno v části Co je instalováno pro třídy IBM MQ pro platformu JMS, a soubor 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 platformu JMS a Proměnné prostředí související s třídami IBM MQ pro jazyk Java.

MQ_JAVA_LIB_PATH

Proměnná prostředí **MQ_JAVA_LIB_PATH** určuje adresář, ve kterém jsou uloženy knihovny IBM MQ classes for JMSa IBM MQ classes for Java . Některé skripty, například IVTRun, které jsou dodávány s proměnnou prostředí IBM MQ classes for JMS nebo IBM MQ classes for Java , používají tuto proměnnou prostředí.

Další informace naleznete v tématu Nastavení proměnných prostředí pro třídy IBM MQ pro platformu JMS a Proměnné prostředí související s třídami IBM MQ pro jazyk Java.

MQ_SET_NODELAYACK

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.

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

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 UNIX V systému UNIX 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 URL jako jedinou hodnotu, ze které lze získat tabulku definic kanálů klienta pro nativní programy, které se připojují jako klienti, tj. aplikace v jazycích C, COBOL nebo C + +.

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

Produkt IBM MQ podporuje načítání tabulky CCDT ze souboru, ftp nebo http URL. Avšak **MQCCDTURL** přijímá pouze hodnotu 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 téma “Přístup URL k tabulce CCDT” na stránce 51.

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 UNIX Pro systémy UNIX 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 UNIX Pro systémy UNIX 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 UNIX V systému UNIX 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 UNIX V systému UNIX and Linux: *datapath*/@ipcc
- Windows V systému Windows: *datapath*\@ipcc
- IBM i V systému IBM i: *datapath*/&ipcc

Nebo:

- Linux UNIX V systému UNIX 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 UNIX /var/mqm na systémech UNIX 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:
  - IBM i Linux UNIX V souboru mqs.ini na adrese IBM i, UNIX 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 URL , která pracuje v kombinaci s proměnnou prostředí MQCHLTAB (viz “Přístup URL k tabulce CCDT” na stránce 51).
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 viz “Umístění pro tabulky CCDT” na stránce 50, “Přístup URL k tabulce CCDT” na stránce 51a Připojení aplikací klienta 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 UNIX V systému UNIX 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 viz “Umístění pro tabulky CCDT” na stránce 50, “Přístup URL k tabulce CCDT” na stránce 51a Připojení aplikací klienta 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 URL. To znamená, že název souboru nemusí být nutně `mqclient.ini`, což usnadňuje umístění souboru do systému souborů připojeného k síti. Další informace naleznete v tématech “IBM MQ MQI client konfigurační soubor mqclient.ini” na stránce 143 a “Umístění konfiguračního souboru klienta” na stránce 145.

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 Instalace IBM MQ classes for .NET Standard.

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 UNIX V systému UNIX 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)
```

MQLICENSE

Linux V 9.1.5

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 provést, naleznete v tématu Přijetí licence na systému 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

Multi

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

Další informace naleznete v tématu Použití protokolů chyb.

MQNAME

Windows

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 téma “Definování lokálního názvu NetBIOS produktu IBM MQ” na stránce 235.

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, přečtěte si téma Co dělat, když produkt MFT nečte vlastnosti úložiště klíčů z konfiguračního souboru úložiště klíčů v systému AMS.

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 UNIX 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 UNIX V systému UNIX 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 viz téma “Vytvoření kanálu připojení klienta v systému IBM MQ MQI client pomocí MQSERVER” na stránce 35.

MQSNOAUT

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.

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

ULW

Proměnná prostředí **MQSSLCRYP** obsahuje řetězec parametrů, který můžete použít ke konfiguraci šifrovacího hardwaru přítomného v systému. Povolené hodnoty jsou stejné jako pro parametr **SSLCRYP** příkazu **ALTER QMGR** .

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

- Linux UNIX Na systémech UNIX and Linux:

```
export MQSSLCRYP=string
```

- Windows Na systémech Windows:

```
SET MQSSLCRYP=string
```

Další informace naleznete v tématu Konfigurace šifrovacího hardwaru v systému UNIX, Linux, and Windows.

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 UNIX Na systémech UNIX 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 kmenovém formátu. Kmenový formát znamená, že obsahuje úplnou cestu a název souboru bez přípony.

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

- Linux UNIX Na systémech UNIX 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 být používán sadou GSKit pro kontroly OCSP.

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

- Linux UNIX Na systémech UNIX 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 být používán sadou GSKit 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 UNIX Například na systémech UNIX 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 UNIX Na systémech UNIX 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

ULW

Produkt IBM MQ můžete nakonfigurovat tak, aby fungoval v souladu se standardem NSA Suite B na platformách UNIX, 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:

- ŽÁDNÉ
- 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.

OMQ_PATH

Proměnná prostředí **OMQ_PATH** uvádí, kde můžete najít sestavu symptomu prvního selhání, pokud se nezdaří vaše třídy automatizace IBM MQ pro skript ActiveX .

OMQ_TRACE

IBM MQ tříd automatizace pro ActiveX (MQAX) obsahuje prostředek trasování, který pomáhá podpoře IBM identifikovat, co se děje, když máte problém. Zobrazuje cesty při spuštění skriptu MQAX. Pokud nemáte problém, spusťte trasování s vypnutým trasováním, abyste se vyhnuli zbytečnému použití systémových prostředků. **OMQ_TRACE** je jedna ze tří proměnných prostředí, které nastavíte pro řízení trasování. Uvedení libovolné hodnoty pro **OMQ_TRACE** zapne prostředek trasování. I když nastavíte **OMQ_TRACE** na 0FF, trasování je stále aktivní.

Další informace viz Řízení trasování pro IBM MQ Třídy automatizace pro ActiveX.

ÚROVNÍ_TRASOVÁNÍ OMQ_TRACE_LEVEL

OMQ_TRACE_LEVEL je jedna ze tří proměnných prostředí, které nastavíte pro řízení trasování pro třídy automatizace IBM MQ pro ActiveX. Nastavuje požadovanou úroveň trasování. Hodnoty větší než 9 nevytvářejí žádné další informace v trasovacím souboru.

Další informace viz Řízení trasování pro IBM MQ Třídy automatizace pro ActiveX.

OMQ_TRACE_PATH

OMQ_TRACE_PATH je jedna ze tří proměnných prostředí, které nastavíte pro řízení trasování pro třídy automatizace IBM MQ pro ActiveX. Nastavuje adresář trasování, do kterého se zapisuje trasovací soubor.

Další informace viz Řízení trasování pro IBM MQ Třídy automatizace pro ActiveX.

ONCONFIG

Proměnná prostředí **ONCONFIG** určuje název konfiguračního souboru serveru Informix . Například na systémech UNIX and Linux použijte toto:

```
export ONCONFIG=onconfig.hostname_1
```

Na systémech Windows použijte toto:

```
set ONCONFIG=onconfig.hostname_1
```

Další informace viz Konfigurace Informix.

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 .

V 9.1.1 Používáte-li produkt IBM MQ classes for XMS .NET Standard, 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.

Související úlohy

"Použití proměnných prostředí IBM MQ" na stránce 60
Pomocí příkazů můžete zobrazit aktuální nastavení nebo resetovat hodnoty proměnných prostředí IBM MQ .

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 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`.

ULW V systému UNIX nebo Linuxobsahuje 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. Další informace viz téma “Konfigurační soubor instalace mqinst.ini” na stránce 142.

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 Service souboru qm.ini” na stránce 128.

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 81.

Umístění adresářů

Linux UNIX V systému UNIX 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 UNIX and Linux , jsou také v registru, protože v systému Windows není žádný soubor `mqinst.ini` (viz "Konfigurační soubor instalace mqinst.ini" na stránce 142).

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 UNIX and Linux

Linux UNIX

```
#*******************************************************************#
#* 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

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 oddílů a atributů souboru mqs.ini

Souhrn atributů oddílů konfiguračního souboru IBM MQ , `mqs.ini`, s odkazy na další informace.

Tabulka 9. Stanzy souboru mqs.ini	
Sekce a atributy	**Popis atributů**
stanza ManagersAllQueue	

Tabulka 9. Stanzy souboru mqs.ini (pokračování)	
Sekce a atributy	**Popis atributů**
DefaultPrefix	Cesta k adresáři `qmgrs` , v němž jsou uložena data správce front.
ULW V 9.1.3 DefaultEphemeralPředpona	Cesta k adresáři, v němž je uchovávána pomíjivá data správce front.
Multi ConvEBCDICNewline	Jak IBM MQ převádí znak NL EBCDIC do formátu ASCII
ApiExitCommon stanza a stanza šablony ApiExit	
Název	Popisný název uživatelské procedury rozhraní API předané do pole Název ExitInfostruktury MQAXP.
funkce	Název vstupního bodu funkce do modulu, který obsahuje kód ukončení rozhraní API.
Modul	Modul obsahující kód ukončení 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.
stanzaDefaultQueueManager	
Název	Název správce front, který zpracovává všechny příkazy, pro které není explicitně určen název správce front.
stanzaExitProperties	
CLWLMode	Zda je uživatelská procedura ukončení práce klastru (CLWL) spuštěna buď v režimu FAST, nebo v režimu SAFE.
stanzaLogDefaults	
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 uvedena v jednotkách 4kB stránek.)
LogType	Typ protokolování, který má být použit správcem front (kruhový nebo lineární).
LogBufferPages	Množství paměti přidělené pro zápis do vyrovnávací paměti a určuje velikost vyrovnávacích pamětí v jednotkách 4kB stránek.
LogDefaultPath	Adresář, ve kterém jsou umístěny soubory žurnálu pro správce front.
LogWriteIntegrity	Metoda, kterou modul protokolování používá ke spolehlivému zápisu záznamů protokolu.
stanzaQueueManager	
Název	Název správce front.

Tabulka 9. Stanzy souboru mqs.ini (pokračování)	
Sekce a atributy	**Popis atributů**
Předpona	Kde jsou uloženy soubory správce front.
Adresář	Název podadresáře pod adresářem `prefix\QMGRS` , kde jsou uloženy soubory správce front.
DataPath	Explicitní cesta k datům, která byla poskytnuta při vytvoření správce front, potlačují předponu a adresář jako cestu k datům správce front.
InstallationName	Název instalace produktu IBM MQ přidružené k tomuto správci front.
V 9.1.3 EphemeralPrefix	Kde je uložena pomíjivá data správce front.
Vysoká dostupnost	Hodnota pro správce replikovaných datových front HA a DR/HA, hodnota je `Replicated`. Atribut se přidá, když se vytvoří správce front a neměl by být změněn.
zotavení z havárie	Přítomný pro replikované správce datových front DR/HA, hodnota je `Replicated`. Atribut se přidá, když se vytvoří správce front a neměl by být změněn.
DRRole	Nachází se pro správce front replikovaných datových front DR a označuje aktuální roli DR správce front. Atribut se přidá, když se správce front vytvoří a aktualizuje pomocí IBM MQ. Nemělo by se měnit ručně.

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: ULW Neodstraňujte adresář `/var/mqm/errors` na systémech UNIX 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.

ULW V 9.1.3 **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** .

Vzhledem k omezením operačního systému je výchozí efemérní předpona omezena na 12 znaků na UNIX and Linux platformáchna 24 znaků.

Produkt **DefaultEphemeralPrefix** není podporován v operačním systému IBM MQ Appliance ani v operačním systému IBM i.

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 88.

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

Tabulka 10. Seznam možných ISO CCSID (pokračování)	
CCSID	**Kódová sada**
1051	roman8

Pokud ASCII CCSID není podmnožina ISO, **ConvEBCDICNewline** standardně zobrazuje NL_TO_LF.

V 9.1.0.2 V 9.1.2 V produktu IBM MQ 9.1.0 Fix Pack 2 a IBM MQ 9.1.2můžete použít 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, TABLEnebo 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 objekt stanza souboru qm.ini” na stránce 106.)

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 stanza správce DefaultQueueManager souboru mqs.ini

Sekce správce DefaultQueueManager uvádí výchozího správce front pro uzel.

Použijte sekci DefaultQueueManager v souboru `mqs.ini` , abyste určili výchozího správce front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností `General` IBM MQ na serveru IBM MQ Explorer .

Název = *default_queue_manager*
Výchozí správce front zpracovává všechny příkazy, pro které není explicitně určen název správce front. Atribut **`DefaultQueueManager`** se automaticky aktualizuje, pokud vytvoříte nového výchozího správce front. Pokud jste neúmyslně vytvořili nového výchozího správce front a poté se chcete vrátit k původnímu správci front, změňte atribut **`DefaultQueueManager`** ručně.

Multi Objekt stanza ExitProperties souboru mqs.ini

Objekt stanza ExitProperties uvádí volby konfigurace použité ukončovacími programy správce front.

Použijte sekci ExitProperties v souboru `mqs.ini` , abyste uvedli volby konfigurace použité ukončovacími programy správce front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `Extended` IBM MQ .

CLWLMode= SAFE (výchozí) |RYCHLÉ
Ukončení pracovní zátěže klustru (CLWL) vám umožňuje určit, která fronta klustru v klustru má být otevřena v rámci odezvy na volání MQI (například `MQOPEN`, `MQPUT`). Uživatelská procedura CLWL se spustí buď v režimu FAST, nebo v režimu SAFE, v závislosti na hodnotě, kterou zadáte na atributu **`CLWLMode`** . Pokud vynecháte atribut **`CLWLMode`** , uživatelská procedura pracovní zátěže klustru se spustí v režimu SAFE.

Bezpečný
Spusťte uživatelskou proceduru CLWL v odděleném procesu od správce front. Toto nastavení je výchozí.

Pokud se vyskytne problém s uživatelskou procedurou CLWL, když je spuštěn v režimu SAFE, nastane následující situace:

- Proces serveru CLWL (amqzlwa0) selže.
- Správce front restartuje proces serveru CLWL.
- Chyba je ohlášena v protokolu chyb. Pokud probíhá volání MQI, obdržíte oznámení ve formě návratového kódu.

Integrita správce front je zachována.

Poznámka: Spuštění uživatelské procedury CLWL v odděleném procesu může ovlivnit výkon.

FAST
Spusťte uživatelskou proceduru klastru vloženou do procesu správce front.

Zadáním této volby zvýšíte výkon tím, že se vyhnete nákladům na přepínání procesu, které jsou přidruženy ke spuštění v režimu SAFE, ale provádí se tak na úkor integrity správce front. Ukončení CLWL byste měli spustit pouze v režimu FAST, jste-li přesvědčeni, že při ukončení vaší uživatelské procedury CLWL nejsou žádné problémy, a vy jste se obzvláště zajímají o výkon.

Pokud se vyskytne problém, když je uživatelská procedura CLWL spuštěna v režimu FAST, správce front selže a vy spustíte riziko, že integrita správce front bude ohrožena.

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 sekce neexistuje, použijí se 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 122.

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 UNIX and Linux” na stránce 83 a “Příklad souboru mqs.ini pro Windows” na stránce 84. Hodnota nula pro atribut `LogBufferPages` znamená 512.

Výchozí předpona, která je určena v souboru “AllQueueSekce správců souboru mqs.ini” na stránce 87, a cesta k protokolu určená pro konkrétního správce front, která je určena v souboru “Sekce protokolu souboru qm.ini” na stránce 122, 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 579.

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* (UNIX 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 UNIX and Linux. Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systému UNIX 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* (UNIX 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 UNIX and Linux. Výchozí číslo je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systému UNIX 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 UNIX 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 574 .

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 574 .

Chcete-li změnit předvolbu, můžete buď upravit atribut LogType , nebo zadat lineární protokolování pomocí příkazu **crtmqm** .

V 9.1.0 V produktu IBM MQ 9.1.0můžete změnit metodu protokolování po vytvoření správce front. Další informace viz migmqlog.

LogBufferStránky = 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 UNIX /var/mqm/log pro systémy UNIX a 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)
Jedná se o výchozí metodu.

Všimněte si, že lze vybrat volbu **DoubleWrite**. Když tak ale uděláte, systém to interpretuje jako volbu **TripleWrite**.

SingleWrite
Měli byste použít **SingleWrite**, pouze pokud 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 “LogWriteIntegrity -pomocí příkazu SingleWrite nebo TripleWrite” na stránce 125.

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.

ULW V 9.1.3 **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.

Související úlohy

“Přidružení správce front k instalaci” na stránce 415
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému UNIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

Windows rozhraní Advanced Configuration and Power Interface (ACPI)

Produkt Windows podporuje standard ACPI (Advanced Configuration and Power Interface). To umožňuje uživatelům produktu Windows s povoleným ACPI hardware zastavit a restartovat kanály, když systém vstoupí do režimu pozastavení a obnoví se z režimu pozastavení.

Použijte stránku vlastností ACPI IBM MQ z IBM MQ Explorer, chcete-li uvést, jak se má IBM MQ chovat, když systém přijme požadavek na pozastavení.

Všimněte si, že nastavení uvedená na stránce vlastností produktu ACPI IBM MQ se použijí pouze tehdy, je-li monitor výstrah spuštěn. Pokud je monitor výstrah spuštěn, je na hlavním panelu zobrazena ikona Monitor výstrah.

DoDialog= Y | N
Zobrazí dialogové okno v době požadavku na pozastavení.

DenySuspend= Y | N
Odepírá požadavek na pozastavení. Používá se, pokud DoDialog= N, nebo pokud DoDialog= Y a dialogové okno nelze zobrazit, například, protože je víko vašeho notebooku zavřeno.

CheckChannelsRunning=Y | N
Zkontroluje, zda jsou spuštěny nějaké kanály. Výsledek může určit výsledek ostatních nastavení.

Následující tabulka ukazuje vliv každé kombinace těchto parametrů:

DoDialog	DenySuspend	Spuštění CheckChannels	Akce
N	N	N	Přijměte požadavek na pozastavení.
N	N	Y	Přijměte požadavek na pozastavení.
N	Y	N	Zamítnout požadavek na pozastavení.
N	Y	Y	Jsou-li některé kanály spuštěny, pozastavte požadavek na pozastavení; pokud žádost nepřijmete.
Y	N	N	Zobrazit dialogové okno (viz Poznámka ; přijmout požadavek na pozastavení). Toto nastavení je výchozí.
Y	N	Y	Pokud nejsou spuštěny žádné kanály, přijměte požadavek na pozastavení; pokud se zobrazí, zobrazí se toto dialogové okno (viz Poznámka). akceptujte požadavek).

Y	Y	N	Zobrazit dialogové okno (Poznámka ; odepřít požadavek na pozastavení).
Y	Y	Y	Pokud nejsou spuštěny žádné kanály, přijměte požadavek na pozastavení; pokud se zobrazí, zobrazí se dialogové okno (Poznámka ; zamítli požadavek).

Poznámka: V případě, že akce má zobrazit dialogové okno, nelze-li dialogové okno zobrazit (například protože je zavřen kryt notebooku), použije se volba DenySuspend k určení, zda je požadavek na pozastavení přijat nebo odepřen.

Multi Konfigurační soubory správce front qm.ini

Konfigurační soubor správce front `qm.ini`obsahuje informace vztahující se ke specifickému správci front.

Pro každého správce front existuje jeden konfigurační soubor správce front. Soubor `qm.ini` se vytvoří automaticky, když je vytvořen správce front, se kterým je asociován.

Poznámka: Další informace o tom, jak a kdy upravovat soubor `qm.ini` a na tom, kdy se všechny změny provedené v souboru uplatní, viz “Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 81.

Z produktů IBM MQ 9.0.4 a IBM MQ 9.0.0 Fix Pack 2příkaz **strmqm** kontroluje syntaxi oddílů CHANNELS a SSL v souboru `qm.ini` před úplným spuštěním správce front, který je mnohem snazší zjistit, co je chybné, a rychle se opraví, pokud **strmqm** zjistí, že soubor `qm.ini` obsahuje chyby. Další informace viz strmqm.

Umístění souborů `qm.ini`

Linux UNIX V systémech UNIX and Linux je soubor `qm.ini` umístěn v kořenovém adresáři adresářového stromu obsazené správcem front. Příklad: Cesta a název konfiguračního souboru pro správce front s názvem QMNAME je:

```
/var/mqm/qmgrs/QMNAME/qm.ini
```

Windows V systémech Windows je umístění souboru `qm.ini` dáno parametrem WorkPath zadaným v klíči `HKLM\SOFTWARE\IBM\WebSphere MQ` . Příklad: Cesta a název konfiguračního souboru pro správce front s názvem QMNAME je následující:

```
C:\ProgramData\IBM\MQ\qmgrs\QMNAME\qm.ini
```

IBM i Soubor `qm.ini` se nachází v souboru *mqmdata directory*`/`*QMNAME*`/qm.ini`, kde *mqmdata directory* je standardně `/QIBM/UserData/mqm` a *QMNAME* je název správce front, pro kterého se použije inicializační soubor.

Poznámka: Můžete změnit *mqmdata directory* v souboru `mqs.ini` .

Název správce front může mít délku až 48 znaků. To však nezaručuje, že název je platný nebo jedinečný. Proto je název adresáře generován na základě názvu správce front. Tento proces je znám jako *transformace názvu*. Popis naleznete v tématu Názvy souborůIBM MQ a Názvy objektů v systému IBM i.

sekce `qm.ini`

Upozornění:

- Toto téma obsahuje odkazy na další informace o stanzách v souboru `qm.ini` . Každá stanza obsahuje informace o parametrech v této stanze, včetně příkladu tam, kde je to vhodné.

- Každá stanza ukazuje platformu nebo platformy IBM MQ for Multiplatforms , na které se tato stanza vztahuje.

V 9.1.4 Multi Automatická konfigurace souboru qm.ini při spuštění

V produktu IBM MQ 9.1.4můžete nakonfigurovat správce front tak, aby automaticky aplikroval obsah souboru nebo sadu souborů, které obsahují potlačení `qm.ini` , na každém spuštění správce front.

Tuto konfiguraci můžete použít k vytvoření konfigurace, kterou lze upravit a automaticky přehrát při příštím spuštění správce front. Například, pokud jsou přepisy `qm.ini` umístěny na připojené jednotce, je možné mít centralizovanou konfiguraci, kde se použije nejnovější verze na každého správce front, jakmile se spustí.

Tuto funkci můžete použít ke zjednodušení vytváření jednotného klastru pomocí funkce automatického klastru. Příklad toho najdete v tématu Vytvoření jednotného klastru z produktu IBM MQ 9.1.4.

Poznámka: Tyto přepisy jsou použity pouze při spuštění správce front a nemohou ovlivnit vytvoření správce front. Například, nemůžete nastavit počet primárních souborů protokolu s touto funkcí.

Než začnete

Můžete použít:

1. Jednotlivý soubor a vytvoření textového souboru obsahujícího změny souboru `qm.ini` .
2. Sada souborů formátu produktu `qm.ini` :
   - Chcete-li identifikovat adresář, ve kterém budou konfigurace existovat, a
   - V tomto adresáři vytvořte soubory, každý s příponou `.ini`, například `qminisettings.ini`.

Soubor nebo soubory musí obsahovat pouze oddíly a nastavení **attribute**=*value* pro položky, které se mění. Chcete-li například aktualizovat atribut **MaxChannels** v sekci Channels, může soubor obsahovat:

```
Channels:
 MaxChannels=1234
```

Všimněte si, že v `qm.ini` přepisu souboru je každý řádek, který má předponu `#` , považován za komentář.

Povolení automatické konfigurace atributů souboru qm.ini

Nový správce front lze konfigurovat pomocí příznaku **-ii** příkazu **crtmqm** a jeho určením na určitém souboru nebo adresáři. Dodaná hodnota se uloží do souboru `qm.ini` pod sekcí AutoConfig jako atribut **IniConfig**.

Chcete-li povolit automatickou konfiguraci MQSC, můžete nakonfigurovat existujícího správce front přidáním atributu stanzy AutoConfig **IniConfig**a odkazováním na platný soubor nebo adresář. Příklad:

```
AutoConfig:
   IniConfig=C:\MQ_Configuration\uniclus.ini
```

Jak funguje automatická konfigurace?

Při spuštění správce front je ověřována konfigurace, která je identifikována atributem 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 nemožnost číst soubor nebo adresář zabrání spuštění správce front spolu s příslušnou chybovou zprávou jak na konzolu, tak i do protokolu chyb správce front.

Při následných restartech, pokud soubor nebo adresář ukazuje na nečitelné, použije se dříve uložený soubor a zpráva se zapíše do protokolu chyb správce front, který jej zvýrazní.

Použijete-li příkaz **strmqm** , obsah souboru `cached.ini` se před vyvoláním správce front použije na soubor `qm.ini` jako přepisy.

To znamená, že v případě správce front v pohotovostním režimu jsou nastavení čtena při zpracování příkazu **strmqm** , nikoli v okamžiku, kdy se správce front stane aktivním.

Jak lze sestavit nahrazující soubor qm.ini ?

Při prvním spuštění konfigurace automatické inicializace a při spuštění správce front je kopie aktuálního souboru `qm.ini` zkopírována do podadresáře `autoconfig` v datovém adresáři správce front jako `base_qm.ini`. Tato úroveň se od této chvíle považuje za základní úroveň.

On every queue manager start, that is, **strmqm** time, the currently active `qm.ini` file is discarded and replaced with a copy of the `base_qm.ini`. Pak se konfigurace ze souboru `cached.ini` použije na tento soubor.

Jakmile je správce front pod automatickou kontrolou konfigurace, všechny změny souboru `qm.ini` by měly být provedeny prostřednictvím souboru nebo souborů, na které se ukazuje, že používá atribut **IniConfig** ve stanze AutoConfig .

Vzhledem k tomu, že se stávající soubor `qm.ini` odstraní při spuštění správce front, použije se na základní řádku správce front pouze konfigurace v dodaném souboru `qm.ini` s použitím atributu **IniConfig** .

Pokud byl objekt stanza nebo atribut změněn pomocí automatické konfigurace inicializace při předchozích spuštění správce front, tyto změny se odstraní, pokud nejsou stále identifikovány v souboru nebo souborech identifikovaných atributem **IniConfig** .

Vzhledem k tomu, že se znovu spustí soubor `qm.ini` při spuštění správce front, znamená to, že všechny ruční změny souboru `qm.ini` budou ztraceny. Pokud opravdu potřebujete provést změnu jako trvalé a nemůžete použít atribut **IniConfig** k provedení této změny, můžete provést jednu z následujících možností:

- Proveďte změnu na samotný soubor `base_qm.ini` .
- Odstraňte soubor `base_qm.ini` .

  Pokud odstraníte tento soubor, `base_qm.ini` se znovu vytvoří při příštím spuštění správce front, a to na základě aktuálního obsahu souboru `qm.ini` . Tento *hards* všechny aktuální změny jako nové úrovně baseline pro budoucí spuštění.

Multi Souhrn sekcí a atributů souboru qm.ini

Souhrn atributů sekcí konfiguračního souboru správce front `qmi.inis` 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.
V 9.1.4 **AutoCluster sekce**	
V 9.1.4 Typ	Typ automatického klastru. Jedinou platnou volbou je volba Uniform, která představuje jednotný klastr.
V 9.1.4 ClusterName	Název automatického klastru.
V 9.1.4 RepositoryName1	Název správce front pro první úplné úložiště v automatickém klastru.
V 9.1.4 Repository1Conname	Hodnota názvu připojení (CONNAME) pro způsob připojení členů automatického klastru ke správci front.
V 9.1.4 RepositoryName2	Název správce front pro druhé úplné úložiště v automatickém klastru.
V 9.1.4 Repository2Conname	Hodnota názvu připojení (CONNAME) pro způsob připojení členů automatického klastru ke správci front.
V 9.1.4 **AutoConfig sekce**	
V 9.1.4 MQSCConfig	Buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.mqsc` použity na správce front při každém spuštění správce front.
V 9.1.4 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.
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.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
AdoptNewMCACheck	Při povolování atributu **AdoptNewMCA** je vyžadován typ kontroly.
V 9.1.0 ChlauthEarlyPřijmout	Pořadí, ve kterém jsou zpracována pravidla ověřování připojení a ověřování kanálu.
PasswordProtection	Místo použití TLS nastavte chráněná hesla ve struktuře MQCSP.
V 9.1.0 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.)
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 UNIX Syslog	Služba syslog, která odesílá nefiltrované zprávy do protokolu syslog pomocí specifikace diagnostických zpráv formátu JSON .
Linux UNIX Ident	Hodnota identifikátoru přidružená k položkám syslog. (podporováno pouze v případě, že je atribut Service nastaven na hodnotu Syslog.)
ExitPath stanza	

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
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.
IBM i Linux UNIX **Sekce systému souborů**	
IBM i Linux UNIX 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.
V 9.1.0 LogManagement	Metoda používaná ke správě oblastí protokolu, a to buď ručně, nebo pomocí správce front.
Windows **LU62 sekce**	
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.
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.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
Windows NumCmds	Počet příkazů, které se mají přidělit.
Windows NumNames	Počet názvů, které se mají přidělit.
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 UNIX **Sekce režimu omezení** [2]	
Linux UNIX 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 UNIX SecurityPolicy	V systému UNIX and Linux, zda správce front používá autorizaci založenou na uživateli nebo na skupině.
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	
AllowOutboundSNI	Uvádí, zda klienti s podporou SNI nastaví SNI na název cílového kanálu IBM MQ pro vzdálený systém při inicializaci připojení TLS.
V 9.1.1 AllowedCipherSpecifikace	Určuje vlastní seznam CipherSpecs , které jsou povoleny pro použití s kanály IBM MQ na platformě Multiplatforms.
V 9.1.4 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.
V 9.1.4 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.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
V 9.1.5 V 9.1.5 OCSPTimeout	Počet sekund čekání na odpovídací modul OCSP při provádění kontroly odvolání.
SSLHTTPProxyName	Buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má být používán sadou GSKit pro kontroly OCSP.
V 9.1.5 V 9.1.5 SSLHTTPConnectTimeout	Počet sekund čekání na úspěšné vytvoření síťového připojení k serveru HTTP při provádění kontroly odvolání.
Sekce dílčího fondu "3" na stránce 104	Tuto sekci vytváří IBM MQ. Neměňte ji.
ShortSubpoolNázev "3" na stránce 104	Název odpovídající adresáři a symbolickému odkazu vytvořenému v adresáři /var/mqm/sockets , který produkt IBM MQ používá pro interní komunikaci mezi běžícími procesy.
Windows **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.
SvrRcvBuffSize	Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech, kterou používá konec serveru kanálu připojení serveru připojení klienta.
V 9.1.0 **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.

Tabulka 11. Sekce souboru qm.ini (pokračování)	
Sekce a atributy	**Popis atributů**
ImplSyncOpenOutput	Minimální počet aplikací, které mají otevřenou frontu pro vložení, než může být povolen implicitní synchronizační bod pro trvalé vložení mimo synchronizační bod.
V 9.1.2 UniformClusterUniformCluster	Název klastru IBM MQ , který používáte jako uniformní klastr.
V 9.1.0.9 OAMLdapConnectČasový limit	Maximální doba v sekundách, po kterou bude klient LDAP čekat na vytvoření připojení TCP k serveru.
V 9.1.0.9 OAMLdapQueryTimeLimit	Maximální doba v sekundách, po kterou bude klient LDAP čekat na přijetí odpovědi na požadavek LDAP ze serveru.
V 9.1.0.15 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.
V 9.1.4 **Sekce Proměnné**	
V 9.1.4 *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.
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 stanza AccessMode souboru qm.ini

Režim přístupu se vztahuje pouze na servery Windows . Sekce AccessMode souboru qm.ini je nastavena pomocí volby `-a [ r]` u příkazu **crtmqm** . Neměňte sekci AccessMode poté, co byl vytvořen správce front.

Použít skupinu přístupů (`-a [ r]`) pomocí volby příkazu **crtmqm** určete skupinu zabezpečení produktu Windows , jejíž členové budou udělen úplný přístup ke všem datovým souborům správce front. Skupina může být buď lokální, nebo globální skupina, v závislosti na použité syntaxi. Platná syntaxe názvu skupiny je následující:

LocalGroup
Název domény\GlobalGroup
GlobalGroup @ Název domény

Než spustíte příkaz **crtmqm** s volbou `-a [ r]` , musíte definovat další skupinu přístupů.

Pokud zadáte skupinu pomocí volby `-ar` místo `-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 oddílu

```
AccessMode:
SecurityGroup=wmq\wmq
```

Související pojmy

“Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows” na stránce 490

“Zabezpečení dat správce sdílených front a adresářů protokolů a souborů v systému Windows” na stránce 487

Související úlohy

“Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462

Související odkazy

crtmqm (vytvoření správce front)

ApiExitLokální objekt stanza souboru qm.ini

Pro server použijte stránku vlastností správce front produktu `Exits` z produktu IBM MQ Explorernebo lokální stanzu ApiExitsouboru `qm.ini` k identifikaci uživatelských procedur rozhraní API pro správce front. V případě klienta upravte lokální sekci ApiExitv souboru mqclient.ini pro identifikaci uživatelských procedur rozhraní API pro správce front.

Na systémech Windows můžete také použít příkaz **amqmdain** ke změně položek pro ukončení rozhraní API. (Chcete-li identifikovat rutiny ukončení rozhraní API pro všechny správce front, použijte stanzy ApiExitCommon a ApiExit, jak je popsáno v tématu “ApiExitCommon a ApiExitstanzas šablony souboru mqs.ini” na stránce 89.)

Všimněte si, že má-li uživatelská procedura rozhraní API pracovat správně, musí být zpráva ze serveru odeslána klientovi, která není konvertována. Poté, co uživatelská procedura rozhraní API zpracuje zprávu, musí být zpráva převedena na klienta. Proto je třeba, abyste instalovali všechny uživatelské procedury pro převod na klientovi.

Další informace o používání těchto atributů najdete v tématu Konfigurace uživatelských procedur rozhraní API.

Název = ApiExit_name
Popisný název uživatelské procedury rozhraní API předané do pole Název ExitInfostruktury MQAXP.

Tento název musí být jedinečný, nesmí být delší než 48 znaků a smí obsahovat pouze platné znaky pro názvy objektů produktu IBM MQ (například názvy front).

Funkce=název_funkce
Název vstupního bodu funkce do modulu, který obsahuje kód ukončení rozhraní API. Tento vstupní bod je funkce MQ_INIT_EXIT.

Délka pole je omezena hodnotou MQ_EXIT_NAME_LENGTH.

Modul = název_modulu
Modul obsahující kód ukončení 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** ve stanze `ExitPath` v souboru `qm.ini` .

Na platformách, které podporují samostatné knihovny s podporou podprocesů, je třeba do modulu uživatelské procedury rozhraní API poskytovat jak nevláknovou, tak i verzi s podporou podprocesů. Svláknová verze musí mít příponu `_r` . Svláknová verze stubu aplikace IBM MQ implicitně připojuje `_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, úvodní a koncové mezery se odstraní, zbývající řetězec se ořízne na 32 znaků a výsledek se předá do ukončení. Pokud tento atribut vynecháte, bude pro ukončení předána výchozí hodnota 32 mezer.

Maximální délka tohoto pole je 32 znaků.

Sequence=sequence_number
Posloupnost, ve které je tato uživatelská procedura rozhraní API volána vzhledem k jiným uživatelským procedurám rozhraní API. Uživatelská procedura s nízkým pořadovým číslem se volá 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 správce front, který z nich má volat jako první. Můžete říci, které bylo voláno po události, tím, že jste čas nebo značku v oblasti ExitChainoznačené jako ExitChainAreaPtr v MQAXP nebo zápisem vašeho vlastního souboru protokolu.

Tento atribut je nepodepsaná číselná hodnota.

V 9.1.4 Multi stanza AutoCluster souboru qm.ini

Sekce AutoCluster se používá, když se správce front začne identifikovat, pokud je klastr členem automatického klastru a může identifikovat úplná úložiště klastru.

Pro sekci AutoCluster jsou povinné následující atributy:

Typ =*Uniform*
Určuje typ automatického klastru a jediná platná volba je *Uniform*(Uniform), který představuje jednotný klastr.

ClusterName=*< Řetězec>*
Název klastru, který je názvem automatického klastru.

Následující atributy jsou volitelné pro sekci AutoCluster , ale musíte je zadat v párech:

RepositoryName1 =*< Řetězec>*
Jedná se o název správce front pro první úplné úložiště v automatickém klastru. Může se jednat o název tohoto správce front nebo o jiný objekt.

Repository1Conname=*< Řetězec názvu připojení >*
Jedná se o hodnotu názvu připojení (CONNAME) pro způsob, jakým se mají členové automatického klastru připojovat k tomuto správci front.

Repository2Name=*< Řetězec>*
Jedná se o název správce front pro druhé úplné úložiště v automatickém klastru. Může se jednat o název tohoto správce front nebo o jiný objekt.

Repository2Conname=*< Řetězec názvu připojení >*
Jedná se o hodnotu názvu připojení (CONNAME) pro způsob, jakým se mají členové automatického klastru připojovat k tomuto správci front.

Příklad oddílu

```
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
Související úlohy
Vytvoření nového jednotného klastru
Použití automatické konfigurace klastru

V 9.1.4 Multi stanza AutoConfig souboru qm.ini

Atributy sekce AutoConfig se často používají jako součást nastavení uniformálních klastrů.

Poznámka: Pro uniformní klastry lze použít pouze sekci AutoCluster .

MQSCConfig=*< cesta>*
Cesta je buď úplná cesta k souboru, nebo cesta k adresáři, kde jsou všechny soubory `*.mqsc` použity na správce front v každém spuštění správce front.

Další informace naleznete v tématu Automatická konfigurace ze skriptu MQSC při spuštění.

IniConfig=*< Path>*
Cesta je buď úplná cesta k souboru, nebo cesta k adresáři, kde se všechny soubory `*.ini` aplikují do souboru `qm.ini` na každém spuštění správce front.

Další informace viz téma “Automatická konfigurace souboru qm.ini při spuštění” na stránce 96.

Příklad oddílu

```
AutoConfig:
        MQSCConfig=/tmp/auto.mqsc
        IniConfig=/tmp/auto.ini
```

Související pojmy
Automatické vyvažování aplikací
Související úlohy
Vytvoření nového jednotného klastru
Použití automatické konfigurace klastru

Multi Sekce Channels souboru qm.ini

Atributy sekce Kanály určují konfiguraci kanálu.

z/OS Tyto informace se nevztahují na IBM MQ for z/OS.

Chcete-li zadat informace o kanálech, použijte stanzu `CHANNELS` v souboru `qm.ini` .

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front produktu IBM MQ Explorer `Channels` .

MaxChannels= 100 (výchozí) |*číslo*
Maximální povolený počet *aktuálních* kanálů.

Výchozí hodnota je 100.

Můžete nastavit **`MaxChannels`** na jinou hodnotu, abyste omezili maximální počet aktuálních kanálů, je-li to potřeba. Pro IBM MQ Applianceje výchozí hodnota 999 999 999 a neměla by se měnit.

MaxActiveChannels = *hodnota MaxChannels_value*
Maximální počet kanálů povolených pro *aktivní* kdykoli. Výchozí hodnota je extrahována z atributu **`MaxChannels`**.

MaxInitiators= 3 (výchozí) |*číslo*
Maximální počet inicializátorů. Výchozí a současně maximální hodnota je 3.

MQIBindType= FASTPATH | STANDARD
Vazba pro aplikace:

Rychlý
Kanály se připojují pomocí rozhraní `MQCONNX` FASTPATH; zde není žádný proces agenta.

STANDARD
Kanály se připojují pomocí STANDARD.

PipeLineLength = 1 |*číslo*
Maximální počet souběžných podprocesů, které kanál použije. Výchozí hodnota je 1. S každou hodnotou větší než 1 se zachází jako s hodnotou 2.

Použijete-li příkaz pipeling, nakonfigurujte správce front na obou koncích kanálu tak, aby měl **`PipeLineLength`** větší než 1.

Poznámka: Potrubování je efektivní pouze pro kanály TCP/IP.

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, v některých případech musí být stávající instance kanálu zastavena dříve, než se může nový spustit. Atribut **`AdoptNewMCA`** umožňuje řídit, které typy kanálů lze v tomto směru ukončit.

Pokud zadáte atribut **AdoptNewMCA** pro konkrétní typ kanálu, ale nový kanál se nespustí, protože odpovídající instance kanálu je již spuštěna:

1. Nový kanál se pokouší zastavit předchozí kanál tak, že jej bude požadovat, aby skončil.
2. Pokud předchozí kanál neodpoví na tento požadavek po uplynutí intervalu čekání **AdoptNewMCATimeout** , ukončí se podproces nebo proces pro předchozí kanál serveru.
3. Pokud předchozí server kanálů nebyl ukončen po kroku 2 a poté, co vyprší interval čekání **AdoptNewMCATimeout** podruhé, produkt IBM MQ ukončí kanál s chybou `CHANNEL IN USE` .

Funkčnost produktu **AdoptNewMCA** se vztahuje na kanály serveru, odesilatele, příjemce a příjemce klastru. V případě odesílatele nebo kanálu serveru může být v přijímajícím správci front spuštěn pouze jedna instance kanálu s konkrétním názvem. V případě přijímacího nebo přijímacího kanálu klastru může být v přijímajícím správci front spuštěn více instancí kanálu s konkrétním názvem, ale v daném okamžiku může být spuštěna pouze jedna instance určitého vzdáleného správce front.

Poznámka: AdoptNewMCA není podporováno u žadatelových nebo serverových kanálů připojení.

Uveďte jednu nebo více hodnot, oddělených čárkami nebo mezerami, z následujícího seznamu:

NO
Funkce `AdoptNewMCA` není povinná. Toto nastavení je výchozí.

SVR
Převzetí kanálů serveru.

SDR
Převzetí odesílacích kanálů.

RCVR
Převzetí přijímacích kanálů.

CLUSRCVR
Převzetí přijímacích kanálů klastru.

ALL
Přijmout všechny typy kanálů kromě kanálů FASTPATH.

Rychlý
Převzetí kanálu v případě, že se jedná o kanál FASTPATH. K tomu dojde pouze v případě, že je zadán také vhodný typ kanálu, například: `AdoptNewMCA=RCVR,SVR,FASTPATH`.

Pozor!: Atribut MCA AdoptNewse může chovat nepředvídatelně s kanály FASTPATH. Dávejte si velkou opatrnost při povolování atributu MCA AdoptNewpro kanály FASTPATH.

AdoptNewMCATimeout= 60 (výchozí) | 1-3600
Doba (v sekundách), po kterou bude nová instance kanálu čekat na ukončení staré instance kanálu. Uveďte hodnotu v rozsahu 1-3600. Výchozí hodnota je 60.

AdoptNewMCACheck = QM | ADDRESS | NAME | ALL
Typ kontroly požadovaný při povolení atributu `AdoptNewMCA` . Je-li to možné, proveďte úplnou kontrolu, abyste ochránili své kanály před vypnutím, neúmyslně nebo neúmyslně. Přinejmenším zkontrolujte, zda se názvy kanálů shodují.

Uveďte jednu nebo více z následujících hodnot oddělených čárkami nebo mezerami v případě *QM*, *NAME*nebo *ALL*:

QM
Zkontrolujte, zda se názvy správců front shodují.

Všimněte si, že samotné jméno správce front se shoduje, nikoli `QMID`.

ADDRESS
Zkontrolujte adresu IP zdroje komunikací. Například adresa TCP/IP.

Poznámka: Hodnoty CONNAME oddělené čárkou se použijí na cílové adresy, a proto nejsou pro tuto volbu důležité.

V případě, že správce front s více instancemi z produktu `hosta` do produktu `hostb`selže, budou všechny odchozí kanály tohoto správce front používat zdrojovou adresu IP produktu `hostb`. Pokud se liší od `hosta`, pak se AdoptNewMCACheck=*ADDRESS* nebude shodovat.

Můžete použít SSL nebo TLS se vzájemným ověřením, abyste zabránili útočníkovi, aby narušil existující běžící kanál. Případně použijte k maskování zdrojové adresy IP řešení typu HACMP s přejímací IP namísto správců front s více instancemi, nebo použijte prostředek pro rozložení zátěže sítě.

NÁZEV
Zkontrolujte, zda se názvy kanálů shodují.

ALL
Zkontrolujte, zda jsou odpovídající názvy správců front, komunikační adresa a odpovídající názvy kanálů.

Výchozí hodnota je `AdoptNewMCACheck=NAME,ADDRESS,QM`.

V 9.1.0 **ChlauthEarlyAdopt = Y (výchozí) | N**

Pořadí, ve kterém jsou zpracovány ověřovací a ověřovací pravidla kanálu, je významným faktorem pro určení kontextu zabezpečení pro připojení klientských aplikací IBM MQ .

Upozornění: Výchozí hodnota, pokud **`ChlauthEarlyAdopt`** není přítomna v souboru qm.ini , je `N`, ale z IBM MQ 9.0.4 jsou všechny správce front vytvořeny s **`ChlauthEarlyAdopt`**=Y automaticky přidány do souboru qm.ini .

`ChlauthEarlyAdopt` přijímá pouze ID uživatelů, která byla poskytnuta správci front pro ověření připojení, je-li parametr ADOPTCTX (YES) nastaven na ověření připojení AUTHINFO objektu ve správci front.

Platné hodnoty pro **`ChlauthEarlyAdopt`** jsou tyto hodnoty:

Y
Kanál ověřuje a přebírá pověření ID uživatele a hesla, která byla poskytnuta aplikací používající ověření připojení správce front, před použitím pravidel pro ověřování kanálu. V tomto režimu provozu se pravidla ověřování kanálu shodují s ID uživatele, které je výsledkem kontrol ověření připojení.

N
Kanál zpožďuje ověření ověření připojení pomocí pověření ID uživatele a hesla, které byly zadány aplikací, dokud nebyla použita pravidla ověření kanálu. Všimněte si, že v tomto režimu provozu, blokování ověření kanálu a pravidla mapování nemohou brát v úvahu výsledky ID uživatele a ověření platnosti hesla.

Například výchozí objekt ověřovacích informací je nastaven na **`ADOPTCTX(YES)`**a uživatel `fred` je přihlášen. Jsou nakonfigurovány následující dvě pravidla CHLAUTH:

```
SET CHLAUTH('MY.CHLAUTH') TYPE(ADDRESSMAP) DESCR('Block all access by
default') ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
SET CHLAUTH('MY.CHLAUTH') TYPE(USERMAP) DESCR('Allow user bob and force
CONNAUTH') CLNTUSER('bob') CHCKCLNT(REQUIRED) USERSRC(CHANNEL)
```

Je zadán následující příkaz se záměrem provést ověření příkazu jako schválený kontext zabezpečení uživatele bob:

```
runmqsc -c -u bob QMGR
```

Ve skutečnosti správce front používá kontext zabezpečení produktu `fred`, nikoli produktu bob, a připojení se nezdaří.

Chcete-li použít kontext zabezpečení produktu bob, produkt **`ChlauthEarlyAdopt`** musí být nastaven na hodnotu Y.

PasswordProtection = `compatible|always|optional|warn`
V produktu IBM MQ 8.0nastavte chráněná hesla ve struktuře MQCSP, raději než pomocí TLS.

Ochrana heslem MQCSP je užitečná pro účely testování a vývoje, protože použití ochrany heslem MQCSP je jednodušší než nastavení šifrování TLS, ale nikoli jako zabezpečené.

Další informace naleznete v tématu Ochrana heslem MQCSP.

V 9.1.0 **IgnoreSeqNumberMismatch = NO (výchozí) | ANO**

Agenti kanálu zpráv (MCA) na obou koncích kanálu každý stále započítávají počet zpráv odeslaných prostřednictvím kanálu za účelem údržby synchronizace. Synchronizace může být ztracena, například pokud je definice kanálu na jednom konci odstraněna a pak znovu vytvořena. Za těchto okolností může být požadováno RESET CHANNEL, aby bylo možné potvrdit, že data synchronizace byla ztracena a aby kanál mohl pokračovat ve spouštění.

Atribut **IgnoreSeqNumberMismatch** musí být nastaven na správci front příjemce.

Ve skutečnosti tento atribut provádí příkaz resetování kanálu na přijímacím kanálu.

Tento atribut řídí, jak správce front zpracuje neshodu pořadového čísla během spouštění kanálu s použitím následujících hodnot:

NO
Během resynchronizace kanálu se kontrolují pořadová čísla kanálů, pokud se dva porty MCV neshodují se stejným pořadovým číslem, bude nahlášena chybová zpráva AMQ9526 a spuštění kanálu se nezdaří.

YES
Během opětovné synchronizace kanálu se kontrolují pořadová čísla kanálů, ale pokud se dva MCA neshodují se stejným pořadovým číslem, bude nahlášena varovná zpráva AMQ9703 a spuštění kanálu bude pokračovat. Tato hodnota atributu by za normálních okolností neměla být potřebná. Je-li známo, že data synchronizace byla ztracena, například během zotavení z havárie, tato volba se vyhýbá nutnosti ručně potvrdit každou neshodu pořadových čísel. Uvedení této hodnoty má podobný efekt pro administrátora, který automaticky vydává **RESET CHANNEL** v odezvě na každou neshodu pořadového čísla.

V 9.1.5 V 9.1.0.5 **ChlauthIgnoreUserCase = N (výchozí) | Y**

Umožňuje správci front vytvořit odpovídající jméno uživatele v rámci pravidel CHLAUTH necitlivé na velikost písmen. Tato volba umožňuje:

- CLNTUSER v pravidlech TYPE (USERMAP) CHLAUTH TYPE (USERMAP), která má být porovnána s necitlivostí
- Pravidla USERLIST v pravidle CHLAUTH TYPE (BLOCKUSER) se porovnávají s rozlišením malých a velkých písmen.

Platné hodnoty pro **ChlauthIgnoreUserCase** jsou tyto hodnoty:

N
Pravidla ověření kanálu se pokusí najít shodu s identifikací uživatele klienta s rozlišováním malých a velkých písmen, například pravidlo určující CLNTUSER ('Fred') se neshoduje s hodnotou 'fred' nebo 'FRED', bude odpovídat pouze identifikátoru uživatele 'Fred'. Toto je výchozí hodnota.

Y
Ověřovací pravidla kanálu se pokusí o shodu s identifikací uživatele klienta s necitlivostí na malá a velká písmena, například pravidlo ověření kanálu s TYPE (USERMAP) nebo TYPE (USERBLOCK), který uvádí CLNTUSER ('Fred'), bude odpovídat všem variantě případu, například identifikátory uživatele 'Fred', 'FRED' a 'fred' se shodují.

Všimněte si, že při ignorování případu uživatelských identifikátorů, když se shodují pravidla ověření kanálu, je možné, aby se shodovala více než jedno pravidlo. Pokud k tomu dojde, pravidlo, které se shoduje, není definováno. Pokud se například uživatel 'fred' připojuje ke správci front prostřednictvím kanálu CLIENT například pomocí následujících pravidel, mohou být mapovány 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 vyhnout jakékoli nejistotě při použití produktu `ChlauthIgnoreUserCase=Y`, vyvarujte se definování pravidel CHLAUTH, která by se překrývala, a výsledkem by bylo odlišné chování při použití shody nerozlišující velikost písmen.

ChlauthIssueVarovat = y
Nastavte tento atribut, pokud chcete, aby byla zpráva AMQ9787 generována při nastavení atributu WARN = YES v příkazu **SET CHLAUTH** .

Příklad oddílu

```
Channels:
   MaxChannels=200
   MaxActiveChannels=100
   MQIBindType=STANDARD
   PipelineLength=2
```

Související pojmy
“Stavy kanálů” na stránce 201
Kanál může být v libovolném okamžiku v některém z mnoha stavů. Některé stavy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

Multi Sekce připojení souboru qm.ini

Stanza Connection definuje výchozí typ vazby.

Chcete-li určit výchozí typ vazby, použijte oddíl Spojení v souboru `qm.ini` .

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front produktu IBM MQ Explorer `Extended` .

Poznámka: Je-li třeba, musíte vytvořit sekci Připojení.

Typ DefaultBindTyp = SHARED (výchozí) |ISOLATED
Je-li parametr **DefaultBindType** nastaven na hodnotu `ISOLATED`, jsou aplikace a správce front spouštěny v samostatných procesech a mezi nimi nejsou sdíleny žádné prostředky.

Je-li parametr **DefaultBindType** nastaven na hodnotu `SHARED`, jsou aplikace a správce front spouštěny v oddělených procesech, ale některé prostředky jsou mezi nimi sdíleny.

Výchozí hodnota je `SHARED`.

Upozornění: DefaultBindType se vztahuje na všechna volání MQCONN a všechny s použitím MQCONNX s parametrem MQCNO_STANDARD_BINDING.

Změna **DefaultBindType** může způsobit snížení výkonu některých aplikací.

Příklad oddílu

```
Connection:
  DefaultBindType=SHARED
```

Protokolování diagnostických zpráv

Protokoly diagnostických zpráv produktu IBM MQ jsou mechanizmem, který umožňuje použití různých komponent systému IBM MQ k hlášení diagnostických zpráv souvisejících s konfigurací IBM MQ a změnami stavu běhového prostředí a s problémy.

Tyto protokoly jsou někdy označovány jako IBM MQ *error logs*, ale vždy obsahovaly IBM MQ informační a varovné zprávy, stejně jako chybové zprávy. Tři primární komponenty produktu IBM MQ , které vykazují tyto protokoly, jsou:

- Správci front
- IBM MQ Klienti
- Zbytek systému IBM MQ

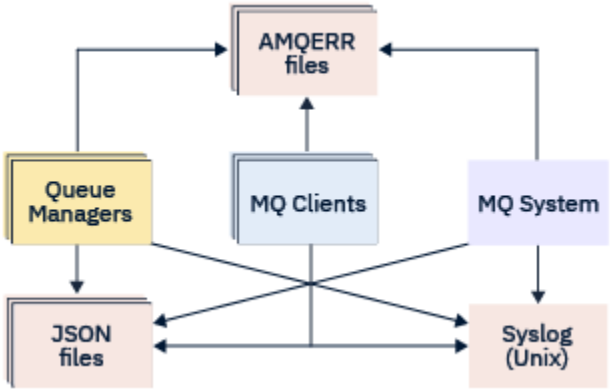
Produkt IBM MQ podporuje hlášení diagnostických zpráv pomocí řady různých metod známých jako *služby diagnostiky zpráv*, což umožňuje přizpůsobit přístup k záznamu a využití těchto informací:

- Soubory protokolu AMQERRnn
- formátované soubory protokolu JSON
- UNIX Systémový protokol ve formátu JSON

Výstup JSON ve formátu IBM MQ je formátován jako objekt JSON v jednom řádku, takže každý jednotlivý řádek protokolu JSON nebo záznam Syslog představuje platný objekt JSON. Protokol jako celek není zapouzdřen jako jediný objekt JSON.

Následující obrázek ukazuje, že správci front, klienti IBM MQ a systém IBM MQ mohou *všechny* hlásit diagnostické zprávy pomocí popsaných metod.

Obrázek 5. Jak různé části produktu IBM MQ mohou hlásit diagnostické zprávy



Jak jsou nakonfigurovány protokoly diagnostiky produktu IBM MQ :

Diagnostické protokoly jsou definovány a přizpůsobeny pomocí oddílů v souboru `qm.ini` , a to zejména pro komponentu IBM MQ , která je vyžaduje. Každý jedinečný koncový bod protokolování je definován pod svým vlastním záhlavím stanzy v souboru INI spolu se všemi přizpůsobeními, která jsou v něm definována. Vlastní nastavení mohou zahrnovat:

- Velikost souborů protokolu, které mají být zalamování, před tím, než dojde k přetočení; nelze použít pro protokol Syslog
- Libovolné filtrování založené na závažnosti zpráv protokolu a
- Libovolné specifické kódy zpráv k potlačení.

Produkt IBM MQ lze nakonfigurovat pro zápis do libovolných nebo všech tří typů koncových bodů protokolování, které umožňují splnění určitých rolí pro jednotlivé role protokolu. Podobně může být definováno více souborových služeb. Příklad:

- Formát JSON usnadňuje analýzu prostřednictvím automatizovaných nástrojů v lokálním prostředí a v prostředí Cloud.
- Výstup systémového protokolu (Syslog) umožňuje komponentám produktu IBM MQ integrovat diagnostické informace do společného umístění protokolování operačního systému v souladu s ostatními produkty v systému.
- Protokolovat koncové body filtrované na základě závažnosti povolení pro konkrétní soubory protokolu k záznamu, například pouze závažné chyby v systému.

Bez ohledu na styl protokolování diagnostiky jsou tradiční diagnostické soubory uchovávané pod adresářem systémového protokolu systému IBM MQ (`/var/mqm/errors/AMQERRnn.log`) a specifickým adresářem protokolu správce front (`/var/mqm/qmgrs/<qmgr_name>/errors/AMQERRnn.log`) vždy napsány tak, aby byly kromě jiné použité konfigurace protokolování vždy napsány.

Pouze pro správce front je možné provést volitelnou konfiguraci těchto povinných protokolů zadáním atributů “Sekce služby diagnostických zpráv” na stránce 115.

Různé oblasti objektu stanza

Další stanzy lze použít na různé oblasti IBM MQ.

Qmgr (qm.ini)
Platí pro zprávy protokolu generované správcem front

Systém (mqs.ini)
Vztahuje se na zprávy protokolu generované systémem. Tato volba není specifická pro správce front, kromě případů, kdy správce front nemůže přistupovat k vlastním protokolům nebo je zapisovat do svých vlastních protokolů.

Šablony (mqs.ini)
Jedna nebo více sekcí jako šablon, které se kopírují do `qm.ini` při vytvoření správce front.

Klient (mqclient.ini)
Vztahuje se na operaci klienta, například **`runmqsc`** v režimu klienta na vzdáleného správce front.

Převod mezi formátováním JSON a tradičně formátovanými protokoly

Příkaz mqrc byl rozšířen tak, aby umožňoval řadu převodů mezi JSON a tradičně formátovanými protokoly a mezi různými jazyky.

Související odkazy

“Sekce služby diagnostických zpráv” na stránce 115
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 114
Sekce chybového protokolu správce front QMErrorLog v souboru `qm.ini` se používá k přizpůsobení provozu a obsahu protokolů chyb produktu IBM MQ .

“Služby diagnostických zpráv” na stránce 118
Mohou být definovány následující služby diagnostických zpráv a jejich specifické atributy služby uvedené ve stanzách DiagnosticSystemMessages, DiagnosticMessages a DiagnosticMessagesve vašich konfiguračních souborech:

Multi *Sekce QMErrorLog*

Sekce chybového protokolu správce front QMErrorLog v souboru `qm.ini` se používá k přizpůsobení provozu a obsahu protokolů chyb produktu IBM MQ .

Služba QMErrorLog je tradiční protokolovací služba diagnostiky IBM MQ používaná k výstupu diagnostických zpráv týkajících se správce front. Služba QMErrorLog běží nepřetržitě a nemůže být vypnuta, ale lze ji do určité míry upravit.

Můžete použít sekci QMErrorLog v souboru `qm.ini` , abyste vyloučili určité zprávy ze zápisu do protokolu chyb správce front. Můžete také potlačit, že zprávy jsou zapisovány do protokolu chyb pro daný časový interval.

Windows Linux Místo úpravy souboru `qm.ini` přímo můžete také použít stránku vlastností správce Extended Queue Manager v produktu IBM MQ Explorer k vyloučení a potlačení zpráv s atributy **Vyloučené zprávy**, **Potlačené zprávy** a **Interval potlačených zpráv** .

Upozornění:

- Windows Produkt IBM MQ Explorer můžete použít k provedení změn pouze tehdy, když používáte lokálního správce front na platformě Windows .
- Objekt stanza QMErrorLog nelze použít pro konfigurační soubor systému IBM MQ , `mqs.ini`nebo konfigurační soubor klienta, obecně nazvaný `mqclient.ini`.

Do sekce QMErrorLog mohou být zahrnuty následující atributy:

ErrorLogVelikost = *maxsize*
Uvádí velikost protokolu chyb správce front, který je zkopírován do zálohy. Hodnota **`maxsize`** musí být v rozsahu 32768 až 2147483648 bajtů. Není-li parametr **`ErrorLogSize`** zadán, bude použita standardní hodnota 33554432 bajtů (32 MB).

Tento atribut můžete použít ke snížení maximální velikosti zpět na předchozí maximum 2 MB, je-li to nutné.

Velikost protokolu můžete nastavit pomocí proměnné prostředí **`MQMAXERRORLOGSIZE`** .

ExcludeMessage= *msgIds*
Určuje zprávy, které nemají být zapsány do protokolu chyb správce front.

Další informace najdete v části ExcludeMessage v příručce “Sekce služby diagnostických zpráv” na stránce 115 .

SuppressMessage= *msgIds*
Určuje zprávy, které jsou zapsány do protokolu chyb správce front pouze jednou za určený časový interval. Je-li stejné ID zprávy uvedeno v souboru `SuppressMessage` a `ExcludeMessage`, zpráva je vyloučena.

Tato volba se nevztahuje na služby diagnostických zpráv definované v produktu `mqclient.ini`. Další informace naleznete v tématu SuppressMessage v příručce “Sekce služby diagnostických zpráv” na stránce 115.

SuppressInterval= *délka*
Určuje časový interval (v sekundách), kdy jsou zprávy uvedené v `SuppressMessage` zapsány do protokolu chyb správce front pouze jednou. *délka* musí být v rozsahu od 1 do 86400 sekund. Není-li parametr `SuppressInterval` zadán, použije se výchozí hodnota 30 sekund.

Příklad oddílu

```
QMErrorLog:
   ErrorLogSize=262144
   ExcludeMessage=7234
   SuppressMessage=9001,9002,9202
   SuppressInterval=30
```

Související pojmy

“Konfigurační soubory správce front qm.ini” na stránce 95
Konfigurační soubor správce front `qm.ini`obsahuje informace vztahující se ke specifickému správci front.

Související odkazy

“Sekce služby diagnostických zpráv” na stránce 115
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 118 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 118

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 114
Sekce chybového protokolu správce front QMErrorLog v souboru `qm.ini` se používá k přizpůsobení provozu a obsahu protokolů chyb produktu IBM MQ .

“Služby diagnostických zpráv” na stránce 118
Mohou být definovány následující služby diagnostických zpráv a jejich specifické atributy služby uvedené ve stanzách DiagnosticSystemMessages, DiagnosticMessages a DiagnosticMessagesve vašich konfiguračních souborech:

Multi *Služby diagnostických zpráv*
Mohou být definovány následující služby diagnostických zpráv a jejich specifické atributy služby uvedené ve stanzách DiagnosticSystemMessages, DiagnosticMessages a DiagnosticMessagesve vašich konfiguračních souborech:

Jsou definovány následující služby diagnostických zpráv:

Soubor
Tato služba odesílá všechny nefiltrované zprávy do souboru podobným způsobem jako služba QMErrorLog . Použije se buď existující textový formát, nebo formát JSON, v závislosti na uvedeném **Format**. Ve výchozím nastavení 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 konfigurované velikosti.

Následující atributy jsou podporovány pouze v oddílu Soubor:

FilePath
Cesta, kam se zapisují soubory protokolu. Předvolba je stejné umístění jako soubory `AMQERR01.log` , to je systém nebo správce front. Cesta musí být absolutní, ale může obsahovat výměnné vložky. Příklad:

+ MQ_Q_MGR_DATA_PATH +
Úplná cesta k nadřízenému adresáři v adresáři diagnostických zpráv správce front. Výchozí hodnoty jsou:

- UNIX Na platformách UNIX and Linux : `/var/mqm/qmgrs/<QM_name>`
- Windows v Windows, `C:\Program Data\IBM\MQ\qmgrs\<QM_name>`

+ MQ_DATA_PATH +
Úplná cesta k nadřízenému adresáři v adresáři systémových diagnostických zpráv. Výchozí hodnoty jsou:

- UNIX Na platformách UNIX and Linux :`/var/mqm`
- Windows V systému Windows: `C:\Program Data\IBM\MQ`

Tuto cestu musíte vytvořit s příslušnými oprávněními, pokud tento adresář nepoužíváte, a to pomocí existujícího adresáře chyb.

FilePrefix
Předpona souborů protokolu. Výchozí hodnota je AMQERR.

FileSize
Velikost, ve které se protokol přetočí. Předvolba je 32MB, jako s vlastností **ErrorLogSize** "Sekce QMErrorLog" na stránce 114, která je sémanticky identická.

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 výchozí nastavení.

Přípona souboru je buď `.LOG` , nebo `.json` založená na nastavení tohoto atributu.

Např. upravte soubor `qm.ini` správce front a přidejte následující stanzu:

```
DiagnosticMessages:
   Service = File
   Name = JSONLogs
   Format = json
   FilePrefix = AMQERR
```

Po restartování bude mít správce front soubory `AMQERR0x.json` v adresáři ERRORS.

Můžete definovat více služeb File Services. To umožňuje konfiguraci tak, jak je zobrazeno v následujících příkladech, kde se zprávy různých značek rozdělují na různé sady protokolů:

```
DiagnosticMessages:
  Name=ErrorsToFile
  Service=File
  Severities=E+
  FilePrefix=OnlyErrors

DiagnosticMessages:
  Name=NonErrorstoFile
  Service=File
  Severities=1 W
  FilePrefix=Information
```

Linux UNIX **Systémový protokol**
Služba Syslog není k dispozici v produktu Windows nebo IBM i

Můžete definovat pouze jednu službu Syslog a služba Syslog odešle všechny nefiltrované zprávy do protokolu syslog pomocí specifikace diagnostických zpráv JSON . Informace se přidají do protokolu syslog v pořadí zobrazeném v tabulce, počínaje parametrem msgID a vloženími.

Závažnost zprávy je mapována na úroveň protokolu systému následujícím způsobem:

Tabulka 12. Mapování závažnosti zpráv na úroveň syslog

Závažnost	**Úroveň**
0	INFORMACE PROTOKOLU
10	VAROV_VAROVÁNÍ
20	LOG_CHYBY
30	LOG_CHYBY
40	VÝSTRAHA PROTOKOLU
50	VÝSTRAHA PROTOKOLU

Následující atribut je podporován pouze ve stanze syslog:

Ident
Definuje hodnotu **ident** přidruženou k položkám protokolu systému. Výchozí hodnota je *ibm-mq*.

Následující příklad zobrazuje chybové zprávy odeslané do protokolu Syslog:

```
DiagnosticMessages:
  Name=ErrorsToSyslog
  Ident=mq
  Service=Syslog
  Severities=E+
```

Další informace o generických atributech stanzy viz “Sekce služby diagnostických zpráv” na stránce 115 .

Notes:

1. Pouze pro službu File Service můžete mít více oddílů, každý s jiným názvem. Pouze definice, použití konečného názvu v posloupnosti, nabývá účinnosti.
2. Změny hodnoty objektu stanza vstoupí v platnost až po restartování správce front.

Multi stanza ExitPath souboru qm.ini

Stanza ExitPath uvádí cestu pro uživatelské programy v systému správce front.

Pomocí objektu stanza `ExitPath` v souboru `qm.ini` zadejte cestu k uživatelským ukončovacím programům v systému správce front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front produktu IBM MQ Explorer `Exits` .

ExitsDefaultCesta = *string*
Atribut Cesta ExitsDefaultuvádí umístění:

- 32bitový kanál se ukončí pro klienty
- 32bitový kanál se ukončí a pro servery existují ukončení konverze dat
- Nekvalifikované soubory načtení přepínače XA

ExitsDefaultPath64= *řetězec*
Atribut ExitsDefaultPath64 uvádí umístění:

- Běžné uživatelské procedury kanálu pro klienty
- Běžné uživatelské procedury kanálu a uživatelské procedury pro převod dat pro servery

- Nekvalifikované soubory načtení přepínače XA

Příklad oddílu

```
ExitPath:
   ExitsDefaultPath=/var/mqm/exits
   ExitsDefaultPath64=/var/mqm/exits64
```

Multi Lokální sekce ExitPropertiesv souboru qm.ini

Lokální stanza 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 produktu IBM MQ Explorer .

Windows Jinou možností je v systému Windows tyto informace zadat pomocí příkazu **amqmdain** .

Standardně je toto nastavení zděděno z atributu **CLWLMode** ve stanze ExitProperties v konfiguraci celého počítače (popsané v části “Objekt stanza ExitProperties souboru mqs.ini” na stránce 90). Změňte toto nastavení pouze v případě, že chcete tohoto správce front nakonfigurovat jiným způsobem. Tuto hodnotu lze u jednotlivých správců front přepsat s použitím atributu režimu pracovní zátěže klastru na stránce vlastností správce front klastru.

Použijte sekci ExitProperties v souboru `mqs.ini` , abyste uvedli volby konfigurace použité ukončovacími programy správce front.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností IBM MQ Explorer `Extended` IBM MQ .

CLWLMode= SAFE (výchozí) |RYCHLÉ
Ukončení pracovní zátěže klastru (CLWL) vám umožňuje určit, která fronta klastru v klastru má být otevřena v rámci odezvy na volání MQI (například `MQOPEN`, `MQPUT`). Uživatelská procedura CLWL se spustí buď v režimu FAST, nebo v režimu SAFE, v závislosti na hodnotě, kterou zadáte na 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 se vyskytne problém s uživatelskou procedurou CLWL, když je spuštěn v režimu SAFE, nastane následující situace:

- Proces serveru CLWL (amqzlwa0) selže.
- Správce front restartuje proces serveru CLWL.
- Chyba je ohlášena v protokolu chyb. Pokud probíhá volání MQI, obdržíte oznámení ve formě návratového kódu.

Integrita správce front je zachována.

Poznámka: Spuštění uživatelské procedury CLWL v odděleném procesu může ovlivnit výkon.

FAST
Spusťte uživatelskou proceduru klastru vloženou do procesu správce front.

Zadáním této volby zvýšíte výkon tím, že se vyhnete nákladům na přepínání procesu, které jsou přidruženy ke spuštění v režimu SAFE, ale provádí se tak na úkor integrity správce front. Ukončení

CLWL byste měli spustit pouze v režimu FAST, jste-li přesvědčeni, že při ukončení vaší uživatelské procedury CLWL nejsou žádné problémy, a vy jste se obzvláště zajímají o výkon.

Pokud se vyskytne problém, když je uživatelská procedura CLWL spuštěna v režimu FAST, správce front selže a vy spustíte riziko, že integrita správce front bude ohrožena.

Příklad oddílu

```
ExitPropertiesLocal:
      CLWLMode=SAFE
```

IBM i Linux UNIX Sekce systému souborů souboru qm.ini

Stanza systému souborů uvádí, zda oprávnění nastavená na protokolech chyb správce front mají zůstat nezměněná, nebo se změní zpět na jejich výchozí hodnoty.

Výchozí oprávnění nastavená u souborů protokolu chyb by měla být užitečná ve většině případů, a proto není třeba, aby je většina administrátorů produktu IBM MQ měnila.

However, your IBM MQ administrator might want to alter the permissions on their error log files, in which case they should set the `Filesystem` stanza option **ValidateAuth**=*Ne.*, which causes the queue manager to leave the permissions unaltered thereafter.

Výchozí chování (bez hodnoty **ValidateAuth**=*Ne*) určuje, že správce front zkontroluje oprávnění k souboru protokolů chyb správce front a změní je zpět na své výchozí hodnoty. Tato kontrola může nastat kdykoli, včetně během ukončení nebo operace spuštění správce front.

Příklad oddílu

```
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 správce front IBM MQ Explorer Log .

Při výchozím nastavení jsou tato nastavení zděděna z nastavení určených pro výchozí nastavení protokolu pro správce front (viz “Sekce LogDefaults souboru mqs.ini” na stránce 91). Tato nastavení změňte pouze v případě, že chcete konfigurovat tohoto správce front jiným způsobem.

Informace o výpočtu velikosti protokolu viz “Výpočet velikosti protokolu” na stránce 579.

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 UNIX 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 UNIX and Linux . Výchozí hodnota je 3.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systémech UNIX and Linux a nesmí být menší než 3.

Hodnota je ověřována při vytváření nebo spouštění správce front. Po vytvoření správce front jej můžete změnit. Změna hodnoty se však neprojeví, dokud nebude správce front restartován a efekt nemusí být okamžitý.

LogSecondaryFiles = 2 (výchozí) |*1-253* (Windows) |*1-509* (systémy UNIX 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 UNIX and Linux . Výchozí číslo je 2.

Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 255 v systému Windowsnebo 511 v systémech UNIX 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 UNIX 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 určenou při vytváření správce front nelze pro správce front změnit.

LogType= CIRCULAR (výchozí) | LINEAR
Typ protokolování, který má používat správce front. Výchozí hodnota je CIRCULAR. Informace o vytvoření správce front s požadovaným typem protokolování naleznete v popisu atributu **LogType** v části “Sekce LogDefaults souboru mqs.ini” na stránce 91 .

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 574 .

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 574 .

Poznámka: Položku **LogType** správce front nelze změnit úpravou tohoto atributu v souboru `qm.ini` . Chcete-li změnit **LogType** správce front, musíte použít příkaz **migmqlog** .

LogBufferStránky = 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 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 UNIX `/var/mqm/log` v systémech UNIX 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` .

V systémech IBM MQ for UNIX a 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)
Jedná se o výchozí metodu.

Všimněte si, že lze vybrat volbu **DoubleWrite**. Když tak ale uděláte, systém to interpretuje jako volbu **TripleWrite**.

SingleWrite
Měli byste použít **SingleWrite**, pouze pokud 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 "LogWriteIntegrity -pomocí příkazu SingleWrite nebo TripleWrite" na stránce 125.

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.

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.

LogWriteIntegrity -pomocí příkazu SingleWrite nebo TripleWrite

Nastavení volby **LogWriteIntegrity** ve stanze Log souboru qm.ini určuje algoritmus používaný zapisovačem protokolu v produktu IBM MQ k zápisu záznamů protokolu do protokolu pro zotavení. Výchozí nastavení je *TripleWrite* a toto nastavení je v téměř každém možném scénáři bezpečné.

Nastavení parametru **LogWriteIntegrity** má libovolný účinek, pouze pokud má být zapsána dílčí stránka protokolu. V případě správce front s rozumným množstvím souběžné aktivity se tento scénář vyskytuje zřídka.

SingleWrite

Volba *SingleWrite* vybere algoritmus, který se za velmi neobvyklých okolností může provést lépe než výchozí nastavení *TripleWrite* . Nastavení *SingleWrite* je bezpečné, pouze pokud základní platforma úložiště může zcela zaručit za všech okolností, že jsou stránky 4KB zapsané synchronně do protokolu pro zotavení produktu MQ atomicky zapsány.

Měli byste použít nastavení *SingleWrite*, pouze pokud se systém souborů nebo zařízení, hostující protokol pro zotavení produktu IBM MQ , explicitně zaručí atomičnost 4KB zápisů. To znamená, že když selže zápis stránky 4KB z jakéhokoli důvodu, měly by být pouze dva možné stavy buď před obrazem, nebo po obrazu, 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, neexistuje žádný významný rozdíl výkonu mezi *SingleWrite* a *TripleWrite*.

V systému s malou souběžností může existovat významná výhoda výkonu pro *SingleWrite*, ale upřednostňovaným řešením je obvykle zvýšit souběžnost, spíše než použít *SingleWrite*.

Všimněte si, že může být obtížné spolehlivě určit atomičnost 4KB zápisů a změny základního softwaru nebo hardwaru mohou způsobit neplatnost jakékoliv takové záruky.

Máte-li jakékoliv pochybnosti o tom, že vaše paměťová infrastruktura nyní poskytuje požadované záruky a v budoucnu za všech okolností, byste měli použít *TripleWrite*.

Windows stanza LU62 souboru qm.ini (pouzeWindows)

Stanza LU62 uvádí konfigurační parametry protokolu SNA LU 6.2 . Tyto parametry přepisují výchozí atributy pro kanály.

Pomocí objektu stanza LU62 v souboru `qm.ini` můžete určit konfigurační parametry protokolu SNA LU 6.2 . Přepisují výchozí atributy pro kanály.

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front produktu IBM MQ Explorer LU6.2 .

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

Library1= *Název DLLName 1*
Název knihovny APPC DLL.

Výchozí hodnota je WCPIC32.

Library2= *DLLName2*
Totéž jako Library1, používá se, pokud je kód uložen ve dvou samostatných knihovnách.

Výchozí hodnota je WCPIC32.

Windows Sekce NETBIOS souboru qm.ini (pouzeWindows)

Sekce NETBIOS v souboru `qm.ini` určuje konfigurační parametry protokolu NetBIOS . Tyto parametry přepisují výchozí atributy pro kanály.

Chcete-li zadat parametry konfigurace protokolu NetBIOS , použijte oddíl NETBIOS v souboru `qm.ini` . Přepisují výchozí atributy pro kanály.

Windows Linux Případně, v systémech Linux (x86 a x86-64) a Windows, použijte stránku vlastností správce front produktu IBM MQ Explorer Netbios.

LocalName= *název*
Název, pod kterým je tento počítač znám v síti LAN.

AdapterNum= 0 (výchozí) | *adapter_number*
Číslo adaptéru sítě LAN. Výchozí je adaptér 0.

NumSess= 1 (výchozí) | *počet_relací*
Počet relací k přidělení. Výchozí hodnota je 1.

NumCmds= 1 (výchozí) | *počet_příkazů*
Počet příkazů k přidělení. 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.

Linux UNIX stanza RestrictedMode souboru qm.ini

Objekt stanza RestrictedMode uvádí název skupiny, která obsahuje členy, kterým je povoleno spouštět aplikace MQI, aktualizovat všechny prostředky IPCC a měnit obsah některých adresářů správce front. Tato stanza se vztahuje pouze na systémy UNIX and Linux .

Sekce RestrictedMode je nastavena pomocí volby **-g** u příkazu **crtmqm** . Pokud nepoužijete volbu **-g** , stanza se nevytvoří v souboru `qm.ini` .

Existují některé adresáře, v rámci kterých aplikace produktu IBM MQ vytvářejí soubory, zatímco jsou připojeny ke správci front v datovém adresáři správce front. Aby aplikace mohly vytvářet soubory v těchto adresářích, mají udělen přístup pro zápis do světa:

- `/var/mqm/sockets/`*`QMgrName`*`/@ipcc/ssem/`*`hostname`*`/`
- `/var/mqm/sockets/`*`QMgrName`*`/@app/ssem/`*`hostname`*`/`
- `/var/mqm/sockets/`*`QMgrName`*`/zsocketapp/`*`hostname`*`/`

kde *QMGRNAME* je název správce front a *hostname* je název hostitele.

Na některých systémech je nepřijatelné udělit všem uživatelům přístup pro zápis do těchto adresářů. Například ti, kteří nepotřebují přístup ke správci front. Omezený režim upravuje oprávnění k adresářům, které ukládají data správce front. K adresářům mohou být poté zpřístupněny pouze členové určené aplikační skupiny. Oprávnění ke sdílené paměti IPC systému System V používaná ke komunikaci se správcem front jsou také upravována stejným způsobem.

Skupina aplikací je název skupiny se členy, kteří mají oprávnění k provedení následujících akcí:

- Spustit aplikace MQI
- Aktualizovat všechny prostředky IPCC
- Změnit obsah některých adresářů správce front

Chcete-li pro správce front použít omezený režim, postupujte takto:

- Tvůrce správce front musí být ve skupině `mqm` a ve skupině aplikací.
- ID uživatele produktu `mqm` musí být ve skupině aplikací.
- Všichni uživatelé, kteří chtějí spravovat správce front, musí být ve skupině `mqm` a ve skupině aplikací.
- Všichni uživatelé, kteří chtějí spustit aplikace IBM MQ , musí být ve skupině aplikací.

Všechny volání MQCONN nebo MQCONNX vydané uživatelem, který není ve skupině aplikací, selže s kódem příčiny MQRC_Q_MGR_NOT_AVAILABLE.

Důležité: Pokud jde o mnoho operačních systémů, musí uživatel, který má být rozeznán, přidávat uživatele do určité skupiny, musí se odhlásit a znovu přihlásit.

Omezený režim pracuje se službou autorizace IBM MQ . Proto musíte také uživatelům udělit oprávnění pro připojení k produktu IBM MQ a k přístupu k prostředkům, které vyžadují pomocí autorizační služby produktu IBM MQ .

ULW Další informace o konfiguraci autorizační služby produktu IBM MQ lze najít v části Nastavení zabezpečení v systémech UNIX, Linux, and Windows.

Omezený režim produktu IBM MQ používejte pouze v případě, že ovládací prvek poskytovaný autorizační službou neposkytuje dostatečnou izolaci prostředků správce front.

Související odkazy
`crtmqm` (vytvoření správce front)

Multi Sekce zabezpečení souboru qm.ini

Sekce Zabezpečení uvádí volby pro OAM (Object Authority Manager).

ClusterQueueAccessControl= RQMName | Xmitq
Nastavte tento atribut, chcete-li zkontrolovat řízení přístupu k frontám klastru nebo plně kvalifikovaným frontám hostovaným na správcích front klastru.

RQMNAME
Profily zkontrolované pro řízení přístupu vzdáleně hostovaných front jsou pojmenované fronty nebo pojmenované profily správce front.

XMITQ
Profily zkontrolované pro řízení přístupu vzdáleně hostovaných front jsou rozlišeny jako `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Výchozí hodnota je `Xmitq` .

Windows **GroupModel=GlobalGroups**
Tento atribut určuje, zda produkt OAM kontroluje globální skupiny při určování členství ve skupině pro uživatele v systému Windows.

Předvolba je nekontrolovat globální skupiny.

GlobalGroups
OAM kontroluje globální skupiny.

Pomocí nastavení `GlobalGroups` příkazy autorizace, **setmqaut**, **dspmqaut**a **dmpmqaut** přijímají názvy globálních skupin; viz parametr **setmqaut** -g .

Poznámka: Nastavení produktu `ClusterQueueAcessControl=RQMName` a vlastní implementace autorizační služby na méně než `MQZAS_VERSION_6` výsledků ve správci front se nespouští. V této instanci buď nastavte `ClusterQueueAcessControl=Xmitq` , nebo upgradujte vlastní autorizační službu na `MQZAS_VERSION_6` nebo vyšší.

Příklad oddílu

```
Security:
      ClusterQueueAccessControl=Xmitq
      GroupModel=GlobalGroups
```

Multi Sekce Service souboru qm.ini

Sekce Service se používá k provedení změn do instalovatelných služeb. Tato stanza obsahuje název služby a počet vstupních bodů definovaných pro službu.

Poznámka: Windows Linux Existují významné důsledky pro změnu instalovatelných služeb a jejich komponent. Z tohoto důvodu jsou instalovatelné služby určené pouze pro čtení v produktu IBM MQ Explorer.

Pro každou komponentu v rámci služby musíte zadat také název a cestu k modulu, který obsahuje kód dané komponenty. K tomu použijte sekci ServiceComponent .

Stanzy **Service** a **ServiceComponent** se mohou vyskytnout v libovolném pořadí a klíče stanzy pod nimi se mohou také vyskytnout v libovolném pořadí. Pro každou z těchto stanz musí být všechny klíče oddílu přítomny. Je-li klíč oddílu duplikován, použije se poslední.

Při spuštění správce front zpracuje všechny položky komponenty služby v konfiguračním souboru postupně. Poté načte uvedený modul komponenty, vyvolá vstupní bod komponenty (která musí být vstupním bodem pro inicializaci komponenty) a předá ji obslužnou rutinu konfigurace.

Název = AuthorizationService (výchozí) |NameService
Název požadované služby.

AuthorizationService
Pro produkt IBM MQje komponenta Authorization Service známá jako správce oprávnění k objektu nebo OAM. Sekce AuthorizationService a její přidružená stanza ServiceComponent se přidávají automaticky při vytvoření správce front. Přidejte další stanzy ServiceComponent ručně.

Linux AIX Následující sekce v konfiguračním souboru správce front definují dvě komponenty autorizační služby v produktu 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
```

Obrázek 6. Stanzy autorizační služby produktu UNIX and Linux v souboru qm.ini

Linux AIX Stanza service component (`MQSeries.UNIX.auth.service`) definuje výchozí komponentu autorizační služby, OAM. Pokud odeberete tuto stanzu a restartujete správce front, bude OAM zablokováno a nebudou provedeny žádné kontroly autorizace.

Windows Atribut `SecurityPolicy` můžete také přidat pomocí služeb produktu IBM MQ . Atribut `SecurityPolicy` se používá pouze v případě, že služba uvedená ve stanze *`Service`* je autorizační služba, to znamená výchozí OAM. Atribut `SecurityPolicy` vám umožňuje uvést zásady zabezpečení pro každého správce front. Možné hodnoty jsou:

`Default`
Uveďte `Default` , pokud chcete, aby se projevila výchozí zásada zabezpečení. Pokud identifikátor zabezpečení produktu Windows (NT SID) není předán OAM pro konkrétní ID uživatele, provede se pokus o získání příslušného SID prohledáváním příslušných databází zabezpečení.

`NTSIDsRequired`
Vyžaduje, aby při provádění kontrol zabezpečení byl při provádění kontroly zabezpečení předán identifikátor SID systému NT.

Windows Stanza Service Component, `MQSeries.WindowsNT.auth.service` definuje výchozí komponentu autorizační služby, OAM. Pokud odeberete tuto stanzu a restartujete správce front, bude OAM zablokováno a nebudou provedeny žádné kontroly autorizace.

NameService
Ve výchozím nastavení není poskytována žádná služba názvů. Požadujete-li službu názvů, musíte přidat sekci `NameService` ručně.

Linux AIX Následující příklady stanz konfiguračního souboru UNIX and Linux pro službu názvů určují komponentu služby názvů, kterou poskytla (fiktivní) společnost 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
```

Obrázek 7. Stanzy služby názvů v souboru qm.ini (pro systémy UNIX and Linux)

EntryPoints= *počet-záznamů*
Počet vstupních bodů definovaných pro službu.

To zahrnuje vstupní body inicializace a ukončení.

Windows **SecurityPolicy= Default |NTSIDsRequired**

V systémech Windows se atribut **SecurityPolicy** použije pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **SecurityPolicy** vám umožňuje uvést zásady zabezpečení pro každého správce front.

Možné hodnoty jsou:

Výchozí
Použijte výchozí zásady zabezpečení, které se mají použít. Pokud identifikátor zabezpečení produktu Windows (NT SID) není předán OAM pro konkrétní ID uživatele, provede se pokus o získání příslušného SID prohledáváním příslušných databází zabezpečení.

NTSIDsRequired
Při provádění kontrol zabezpečení předejte SID systému NT pro OAM.

Další informace viz ID zabezpečení produktuWindows (SIDs).

Viz též Configuring authorization service stanza: Windows systems.

Linux UNIX **SecurityPolicy= uživatel|skupina|výchozí**

V systémech UNIX and Linux hodnota určuje, zda správce front používá autorizaci založenou na uživateli nebo na základě skupin. Hodnoty nejsou citlivé na velikost písmen.

Pokud nezahrnete atribut **SecurityPolicy** , použije se `předvolba` , která používá autorizaci založenou na skupině.

Aby se změny projevily, restartujte správce front. Viz též Configuring authorization service stanza: Windows systems.

SharedBindingsUserId= *typ-uživatele*

Atribut **SharedBindingsUserId** se použije 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 uvést, zda je pole *UserIdentifier* ve struktuře *IdentityContext* , z funkce MQZ_AUTHENTICATE_USER, efektivní ID uživatele nebo skutečné ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu MQZ_AUTHENTICATE_USER-Authenticate user.

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** se použije pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **FastpathBindingsUserId** se používá pouze s vazbou na vazby zkrácené cesty. Tato hodnota vám umožňuje uvést, zda je pole *UserIdentifier* ve struktuře *IdentityContext* , z funkce MQZ_AUTHENTICATE_USER, efektivní ID uživatele nebo skutečné ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu MQZ_AUTHENTICATE_USER-Authenticate user.

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** se použije pouze v případě, že uvedená služba je výchozí autorizační službou, tj. OAM. Atribut **IsolatedBindingsUserId** se používá pouze ve vztahu k izolovaným vazbám. Tato hodnota vám umožňuje uvést, zda je pole *UserIdentifier* ve struktuře *IdentityContext* , z funkce MQZ_AUTHENTICATE_USER, efektivní ID uživatele nebo skutečné ID uživatele.

Informace o funkci MQZ_AUTHENTICATE_USER naleznete v tématu MQZ_AUTHENTICATE_USER-Authenticate user.

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 najdete v tématu Instalovatelné služby a komponenty pro produkt UNIX, Linux, and Windows.

Další informace o službách zabezpečení obecně najdete v tématu Nastavení zabezpečení v systémech UNIX and Linux.

Příklad oddílu

```
Service:
   Name=AuthorizationService
   EntryPoints=14
```

Související pojmy
Instalovatelné služby a komponenty pro systémy AIX, Linuxa Windows
Související odkazy
Instalovatelné služby a komponenty v systému IBM i
Referenční informace o instalovatelných službách

Multi stanza ServiceComponent souboru qm.ini

Objekt stanza ServiceComponent uvádí informace pro komponentu služby. Když přidáváte novou instalovatelnou službu, musíte uvést informace o komponentě služby. Sekce autorizační služby je standardně přítomná a přidružená komponenta, OAM, je aktivní.

Stanzy **Service** a **ServiceComponent** se mohou vyskytnout v libovolném pořadí a klíče stanzy pod nimi se mohou také vyskytnout v libovolném pořadí. Pro každou z těchto stanz musí být všechny klíče oddílu přítomny. Je-li klíč oddílu duplikován, použije se poslední.

Při spuštění správce front zpracuje všechny položky komponenty služby v konfiguračním souboru postupně. Poté načte uvedený modul komponenty, vyvolá vstupní bod komponenty (která musí být vstupním bodem pro inicializaci komponenty) a předá ji obslužnou rutinu konfigurace.

Služba = *název_služby*
Název požadované služby. Musí odpovídat hodnotě zadané v atributu Name v informacích o konfiguraci služby.

Název = *název_komponenty*
Popisný název komponenty služby. Musí být jedinečný a obsahovat pouze znaky, které jsou platné pro názvy objektů produktu IBM MQ (například názvy front). Tento název se vyskytuje ve zprávách operátora generovaných službou. Doporučujeme, aby tento název začal ochrannou známkou společnosti nebo obdobným rozlišovacím řetězcem.

Modul = *název_modulu*
Název modulu, který má obsahovat kód pro tuto komponentu. Musí se jednat o úplný název cesty.

ComponentDataVelikost = *velikost*
Velikost (v bajtech) oblasti dat komponenty předaného komponentě při každém volání. Uveďte nulu, pokud nejsou požadována žádná data komponenty.

Příklad oddílu

```
ServiceComponent:
   Service=AuthorizationService
   Name=MQSeries.UNIX.auth.service
   Module=amqzfu
   ComponentDataSize=0
```

Další příklady zobrazující stanzu AuthorizationService a přidruženou stanzu ServiceComponent a sekci NameService a přidruženou sekci ServiceComponent viz “Sekce Service souboru qm.ini” na stránce 128.

Související pojmy

Instalovatelné služby a komponenty pro systémy AIX, Linuxa Windows

Související odkazy

“Sekce Service souboru qm.ini” na stránce 128
Sekce Service se používá k provedení změn do instalovatelných služeb. Tato stanza obsahuje název služby a počet vstupních bodů definovaných pro službu.

Instalovatelné služby a komponenty v systému IBM i

Referenční informace o instalovatelných službách

Windows Sekce SPX souboru qm.ini (pouzeWindows)

Stanza SPX určuje parametry konfigurace protokolu SPX. Tyto parametry přepisují výchozí atributy pro kanály.

Chcete-li zadat parametry konfigurace protokolu SPX, použijte stanzu SPX v souboru `qm.ini` .

Windows Linux Případně v systémech Linux (x86 a x86-64) a Windowspoužijte stránku vlastností správce front produktu IBM MQ Explorer SPX .

Socket = 5E86 (výchozí) | *socket_number*
Číslo soketu SPX v hexadecimální notaci. Výchozí hodnota je X'5E86'.

BoardNum= 0 (výchozí) | *adapter_number*
Číslo adaptéru LAN. Výchozí je adaptér 0.

KeepAlive= NE | ANO
Vypněte funkci KeepAlive zapnutou nebo vypnutou.

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

Library1= *DLLName1*
Název knihovny SPX DLL.

Výchozí hodnota je WSOCK32.DLL.

Library2= *DLLName2*
To samé jako LibraryName1, použito, pokud je kód uložen ve dvou samostatných knihovnách.

Výchozí hodnota je WSOCK32.DLL.

ListenerBacklog= číslo
Potlačit výchozí počet nevyřízených požadavků pro modul listener SPX.

Při příjmu na SPX je nastaven maximální počet neprovedených požadavků na připojení. Tento stav lze považovat za seznam požadavků čekajících na soket protokolu SPX pro příjem požadavků, které čekají na příjem požadavku. Výchozí hodnoty nevyřízených požadavků listeneru jsou zobrazeny v Tabulka 13 na stránce 133.

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 zobrazená hodnota. Použijte k tomu, abyste se vyvarovali dosažení limitu připojení.

Naopak, některé operační systémy mohou omezit velikost nevyřízených požadavků SPX, takže efektivní nevyřízené požadavky SPX by mohly být menší, než se zde požadovalo.

Pokud počet nevyřízených požadavků dosáhne hodnot zobrazených v Tabulka 13 na stránce 133, je spojení SPX odmítnuto a kanál nelze spustit. V případě kanálů pro zprávy se tyto výsledky ve kanálu přejdou do stavu ZOPAKOVÁNÍ a později se znovu pokusí o připojení. V případě připojení klienta obdrží klient kód příčiny MQRC_Q_MGR_NOT_AVAILABLE z hodnoty `MQCONN` a měl by pokus o 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.

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.

V 9.1.1 **AllowedCipherSpecifikace =*název|seznam názvů*| ALL**

Určuje vlastní seznam CipherSpecs , které jsou povoleny pro použití s kanály IBM MQ na platformě Multiplatforms.

- jeden název CipherSpec nebo
- Čárkami oddělený seznam názvů IBM MQ CipherSpec , které chcete znovu povolit, nebo
- Speciální hodnota ALLpředstavující 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 tématu Povolení CipherSpecs.

ULW V 9.1.4 **AllowTLSV13 =Y | YES | T | TRUE| N | NO | F | FALSE**

Určuje, zda může správce front používat specifikaci TLS 1.3 CipherSpecs.

- Y, YES, Tnebo TRUE: 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 (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.

ULW V 9.1.4 **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.

ULW V 9.1.5 **OCSPTimeout=** ***number***

Počet sekund čekání na odpovídací modul OCSP při provádění kontroly odvolání.

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 být použit sadou GSKit 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.

Solaris AIX Pro 32bitové klienty na platformách AIX, a Solaris SPARC, může 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.

ULW V 9.1.5 **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
      SSLHTTPConnectTimeout=0
```

Notes:

- Výchozí hodnota parametru **OutboundSNI** je Kanál.
- V 9.1.1 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
- V 9.1.4 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.

Multi Oddíl podfondu souboru qm.ini

Tato stanza je vytvořena IBM MQ. Neměňte jej.

Oddíl Subpool a atribut **ShortSubpoolName** v rámci této stanzy jsou při vytváření správce front zapisovány automaticky produktem IBM MQ . IBM MQ zvolí hodnotu pro **ShortSubpoolName**. Tuto hodnotu neměňte.

Název odpovídá adresáři a symbolickému odkazu vytvořenému uvnitř adresáře `/var/mqm/sockets` , který produkt IBM MQ používá pro interní komunikaci mezi spuštěnými 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.

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 136.

Tabulka 14. Výchozí nevyřízené požadavky na připojení (TCP)

Platforma	**Výchozí hodnota ListenerBacklog**
Windows Windows Server	100
Linux Linux	100
Solaris Solaris	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 136, 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 138.

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 138.

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 138.

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 138.

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 138.

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 138).

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.

V 9.1.0 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=0FF`.

V 9.1.2 **UniformClusterNázev =*název klastru***
Název klastru IBM MQ , který používáte jako jednotný klastr.

V 9.1.0.9 **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.

V 9.1.0.9 **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 9.1.0.15 **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 .

Příklad stanza

V 9.1.0.15

```
TuningParameters:
       SuppressDspAuthFail=NO
       ImplSyncOpenOutput=2
       OAMLdapConnectTimeout=60
       OAMLdapQueryTimeLimit=60
       OAMLdapResponseWarningTime=10
       ExpiryInterval=300
```

Související pojmy
Implicitní synchronizační bod

V 9.1.4 Multi Stanza Variables souboru qm.ini

Stanza Proměnné uvádí proměnné konfigurace pro použití s automatickými uniformálními klastry.

Atributy uvedené v sekci Proměnné můžete použít během automatické konfigurace klastru v polích CONNAME a názvu kanálu MQSC kanálu příjemce klastru. Konfigurační proměnné nelze použít v žádném jiném prvku skriptu MQSC.

atribut=hodnota
Uvádí název a přidruženou hodnotu pro použití jako vložení během definic MQSC.

Dvojice hodnot *atribut=hodnota* lze při vytváření správce front zadat pomocí volby příkazového řádku **-iv** v příkazu **crtmqm** .

Příklad oddílu

```
Variables:
       CONNAME=127.0.0.1(1414)
```

Související pojmy
Automatické vyvažování aplikací
Související úlohy
Vytvoření nového jednotného klastru
Související odkazy
Použití automatické konfigurace klastru

Multi stanza XAResourceManager souboru qm.ini

Objekt stanza XAResourceManager určuje informace o správcích prostředků zapojených do globálních transakcí koordinovaných správcem front.

Použijte sekci XAResourceManager v souboru `qm.ini` , abyste uvedli informace o správcích prostředků zapojených do globálních pracovních jednotek koordinovaných správcem front.

Windows Linux Případně můžete na stránce Linux (x86 a x86-64) a Windowspoužít stránku vlastností správce front správce prostředků XA IBM MQ Explorer .

Ručně přidejte informace o konfiguraci správce prostředků XA pro každou instanci správce prostředků, která se podílí na globálních pracovních jednotkách; nejsou zadány žádné výchozí hodnoty.

Další informace o atributech správce prostředků najdete v tématu Koordinace databáze .

Název = *název* (povinné)
Tento atribut identifikuje instanci správce prostředků.

Hodnota `Name` může být dlouhá až 31 znaků. Můžete použít název správce prostředků, jak je definován ve své struktuře XA-switch. Pokud však používáte více než jednu instanci téhož správce prostředků, je nutné pro každou instanci vytvořit jedinečný název. Jedinečnost je možné zajistit zahrnutím názvu databáze do řetězce `Name` , například.

Produkt IBM MQ používá hodnotu `Name` ve zprávách a ve výstupu příkazu `dspmqtrn` .

Neměňte název instance správce prostředků nebo odstraňte její položku z informací o konfiguraci poté, co je přidružený správce front spuštěn a že je název správce prostředků v platnosti.

SwitchFile= *název* (povinné)
Úplný název zaváděcího souboru obsahujícího strukturu přepínačů XA správce prostředků.

Používáte-li 64bitového správce front s 32bitovými aplikacemi, měla by hodnota `name` obsahovat pouze základní název zaváděcího souboru obsahujícího strukturu přepínačů XA správce prostředků.

32bitový soubor se načte do aplikace z cesty uvedené v cestě `ExitsDefaultPath`.

64bitový soubor bude načten do správce front z cesty určené parametrem `ExitsDefaultPath64`.

XAOpenString= *řetězec* (volitelné)
Řetězec dat, který má být předán do vstupního bodu xa_open správce prostředků. Obsah řetězce závisí na samotném správci prostředků. Řetězec může například identifikovat databázi, ke které má tato instance správce prostředků přístup. Další informace o definování tohoto atributu najdete v tématu:

- Přidání konfiguračních informací správce prostředků pro produkt Db2
- Přidání konfiguračních informací správce prostředků pro Oracle
- Přidání konfiguračních informací správce prostředků pro Sybase
- Přidání konfiguračních informací správce prostředků pro produkt Informix

a v dokumentaci správce prostředků vyhledejte příslušný řetězec.

XACloseString= *řetězec* (volitelné)
Řetězec dat, který má být předán do vstupního bodu xa_close správce prostředků. Obsah řetězce závisí na samotném správci prostředků. Další informace o definování tohoto atributu najdete v tématu:

- Přidání konfiguračních informací správce prostředků pro produkt Db2

- Přidání konfiguračních informací správce prostředků pro Oracle
- Přidání konfiguračních informací správce prostředků pro Sybase
- Přidání konfiguračních informací správce prostředků pro produkt Informix

a nahlédněte do dokumentace k databázi pro příslušný řetězec.

ThreadOfControl=THREAD | PROCESS

Windows Tento atribut je povinný pro produkt Windows. Správce front používá tuto hodnotu pro serializaci, když potřebuje volat správce prostředků z jednoho z jeho vlastních procesů s více podprocesy.

Podproces
Správce prostředků je plně *informován o podprocesu*. Ve vícevláknovém procesu produktu IBM MQ lze volání funkce XA provést pro externího správce prostředků z více podprocesů současně.

PROCESS
Správce prostředků není *bezpečný pro podproces*. V procesu IBM MQ s podporou podprocesů lze ve správci prostředků provést pouze jedno volání funkce XA v daném okamžiku.

Položka **ThreadOfControl** se nevztahuje na volání funkcí XA vydaná správcem front v procesu aplikace s podporou podprocesů. Obecně platí, že aplikace, která má souběžné jednotky práce na různých podprocesech, vyžaduje, aby tento režim operace byl podporován každým správcem prostředků.

Příklad oddílu

```
XAResourceManager:
   Name=DB2 Resource Manager Bank
   SwitchFile=/usr/bin/db2swit
   XAOpenString=MQBankDB
   XACloseString=
   ThreadOfControl=THREAD
```

Poznámka: Maximální počet oddílů XAResourceManager je omezen na 255. Měli byste však použít pouze malý počet oddílů, abyste se vyvarovali snížení výkonu transakce.

IBM i Příklad souboru qm.ini pro IBM i

Příklad, který ukazuje, 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
```

ULW Konfigurační soubor instalace mqinst.ini

V systémech UNIX nebo Linuxobsahuje konfigurační soubor instalace `mqinst.ini`informace o všech instalacích produktu IBM MQ . V systému Windowsjsou informace o konfiguraci instalace v registru.

Umístění souboru `mqinst.ini`

Linux UNIX

Soubor `mqinst.ini` se nachází v adresáři `/etc/opt/mqm` na systémech UNIX and Linux . Obsahuje informace o instalaci, je-li k dispozici, o primární instalaci a o následujících informacích pro každou instalaci:

- Název instalace
- Popis instalace
- Identifikátor instalace
- Instalační cesta

Důležité: Soubor `mqinst.ini` nesmí být upravován nebo odkazován přímo, protože jeho formát není pevný a mohl by se změnit.

Je automaticky nastaven identifikátor instalace, pouze pro vnitřní použití, a nesmí být změněn.

Místo úpravy souboru `mqinst.ini`přímo, musíte použít následující příkazy k vytvoření, odstranění, dotazu a úpravě hodnot v souboru:

crtmqinst pro vytvoření položek.
dltmqinst k odstranění položek.
dspmqinst pro zobrazení položek.
setmqinst pro nastavení položek.

Informace o konfiguraci instalace v systému Windows

Windows

V Windowsnení žádný soubor `mqinst.ini` . Informace o konfiguraci instalace jsou uloženy v registru a jsou umístěny v následujícím klíči:

```
HKLM\SOFTWARE\IBM\WebSphere MQ\Installation\InstallationName
```

Důležité: Tento klíč nesmí být upravován 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 k dispozici příkazy **`crtmqinst`** a **`dltmqinst`** . Procesy instalace a odinstalace manipulují s vytvářením a odstraňováním požadovaných položek registru.

Multi IBM MQ MQI client konfigurační soubor mqclient.ini

Klienty konfigurujete 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:

- ULW UNIX, 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 145.

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 146.

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).

V 9.1.2 Zde je příklad konfiguračního souboru klienta pro Continuous Delivery z IBM MQ 9.1.2:

```
#* 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
```

Zde je příklad konfiguračního souboru klienta pro verzi IBM MQ 9.1.0 Long Term Support a Continuous Delivery před IBM MQ 9.1.2:

```
#* 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)
```

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

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

“Kteří klienti IBM MQ mohou číst každý atribut” na stránce 146
Většina atributů v konfiguračním souboru IBM MQ MQI client může být použita klientem C a nespravovanými klienty .NET . Existují však některé atributy, které nejsou čteny spravovanými klienty .NET a XMS .NET nebo klienty, kteří používají buď IBM MQ classes for Java , nebo IBM MQ classes for JMS.

Související odkazy

“Umístění konfiguračního souboru klienta” na stránce 145
Konfigurační soubor IBM MQ MQI client lze zadržet v několika umístěních.

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 řetězcem `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 Windows, UNIX and Linux .

   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 Proměnné prostředí.

z/OS Platformu z/OS nelze použít ke spuštění klientů IBM MQ . Proto soubor `mqclient.ini` v systému IBM MQ for z/OSneexistuje.

- Linux UNIX Na systémech UNIX and Linux je adresář `/var/mqm`
- Windows Na platformách Windows konfigurujete 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 UNIX Pro klienty C na platformách UNIX 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.

Kteří klienti IBM MQ mohou číst každý atribut

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

Tabulka 15. Které atributy se vztahují na každý typ klienta

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
stanza CHANNELS						
CCSID	Kódované číslo znakové sady, které má být použito.	Ano	Ne	Ne	Ano	Ano
ChannelDefinition	Cesta k adresáři se souborem obsahujícím tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
ChannelDefinition	Název souboru obsahujícího tabulku definic kanálů klienta.	Ano	Ne	Ne	Ano	Ano
ReconDelay	Administrativní volba pro konfiguraci prodlevy opětného připojení pro klientské programy, které se mohou automaticky znovu připojit.	Ano	Ne	Ano	Ano	Ano
DefRecon	Administrativní volba, která umožní klientským programům automaticky znovu navázat spojení nebo zakázat automatické opětovné připojení klientského programu, který byl napsán tak, aby se automaticky znovu připojil.	Ano	Ne	Ano	Ano	Ano
MQReconnectTimeout	Časový limit v sekundách, který se má znovu připojit ke klientovi.	Ano	Ne	Ne	Ano	Ne

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
ParametryServerConnectionParms	Umístění serveru IBM MQ a komunikační metoda, která má být použita.	Ano	Ne	Ne	Ano	Ano
Put1DefaultAlwaysSync	Řídí chování volání funkce MQPUT1 s volbou `MQPMO_RESPONSE_AS_Q_DEF`.	Ano	Ano	Ano	Ano	Ano
PasswordProtection	Umožňuje nastavit chráněná hesla ve struktuře MQCSP raději než pomocí SSL nebo TLS.	Ano	Ano	Ano	Ano	Ano
ClientExit-stanza cesty						
ExitsDefaultPath	Určuje umístění 32bitového kanálu pro klienty.	Ano	Ano	Ano	Ano	Ano
ExitsDefaultPath64	Určuje umístění 64bitových kanálů kanálů pro klienty.	Ano	Ano	Ano	Ano	Ano
JavaExitsClassPath	Hodnoty, které mají být přidány do cesty ke třídě při spuštění uživatelské procedury produktu Java .	Ne	Ano	Ano	Ne	Ne

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	Popis	C a nespravováno .NET	Java	JMS	Spravované. NET	Spravované XMS .NET
V 9.1.2 V 9.1.2 **Sekce připojení**						
ApplName	Název aplikace určený v konfiguračním souboru klienta.	Ano	Ne	Ne	Ne	Ne
stanza JMQI						
useMQCSPauthentication	Řídí, zda aplikace IBM MQ classes for Java a IBM MQ classes for JMS mají při ověřování u správce front používat režim kompatibility nebo režim ověřování MQCSP.	Ne	Ano	Ano	Ne	Ne
stanzaMessageBuffer						
MaximumSize	Velikost vyrovnávací paměti dopředného čtení v kilobajtech, v rozsahu od 1 do 999 999.	Ano	Ano	Ano	Ano	Ano
PurgeTime	Interval, v sekundách, po jehož uplynutí jsou vyprázdněny zprávy ponechané ve vyrovnávací paměti dopředného čtení.	Ano	Ano	Ano	Ano	Ano

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

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

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
Sekce zabezpečení						
DisableClientAMS	Zakáže nebo povolí AMS pro připojení klienta ke správci front.	Ano	Ano	Ano	Ne	Ne
Sekce SSL						
AllowOutboundSNI	Uvádí, zda klienti podporující SNI nastaví SNI na cílový název kanálu IBM MQ na vzdálený systém při inicializaci připojení TLS.	Ano	Ne	Ne	Ne	Ne
V 9.1.4 AllowTLSV13	Zda je správce front schopen použít 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 pojmenované v rozšířeních certifikátu bodu CrlDistribution.	Ano	Ne	Ne	Ne	Ne
CertificateLabel	Jmenovka certifikátu pro definici kanálu.	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
CertificateVal	Určuje typ použitého ověření certifikátu.	Ano	Ne	Ne	Ne	Ne
ClientRevocation-kontroly	Určuje, jak je kontrola odvolání certifikátů konfigurována, pokud volání connect klienta používá kanál SSL/TLS.	Ano	Ne	Ne	Ne	Ne
EncryptionPolicySuiteB	Určuje, zda kanál používá šifrování vyhovující standardu Suite-B a jaká úroveň síly se má použít.	Ano	Ne	Ne	Ne	Ne
V 9.1.4 VelikostMinimumRSAKey	Uvádí minimální velikost klíče, kterou musí mít certifikáty RSA, aby mohly být přijaty.	Ano (klienti C/C++)	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
Ověření OCSPAuthentication	Definuje chování produktu IBM MQ , je-li protokol OCSP povolen a kontrola odvolání OCSP není schopna určit stav odvolání certifikátu.	Ano	Ne	Ne	Ne	Ne
OCSPCheckExtensions	Řídí, zda produkt IBM MQ funguje na rozšíření certifikátu AuthorityInfo Access.	Ano	Ne	Ne	Ne	Ne
SSLCryptoHardware	Nastaví řetězec parametrů požadovaný ke konfiguraci kryptografického hardwaru PKCS #11 přítomným na systému.	Ano	Ne	Ne	Ne	Ne
SSLFipsRequired	Určuje, zda mají být použity pouze algoritmy certifikované podle standardu FIPS, je-li šifrování prováděno v produktu IBM MQ.	Ano	Ne	Ne	Ne	Ne

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
SSLHTTPProxyName	Řetězec je buď název hostitele, nebo síťová adresa serveru proxy HTTP, který má sada GSKit použít pro kontroly OCSP.	Ano	Ne	Ne	Ne	Ne
SSLKeyRepository	Umístění úložiště klíčů, které obsahuje digitální certifikát uživatele, v kmenového formátu.	Ano	Ne	Ne	Ne	Ne
PočetSSLKeyResetCount	Počet nezašifrovaných bajtů odeslaných a přijatých na kanál SSL nebo TLS, než je znovu vyjednán tajný klíč.	Ano	Ne	Ne	Ne	Ne
Sekce TCP						
ClntRcvBuffSize	Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.	Ano	Ano	Ano	Ano	Ano

Tabulka 15. Které atributy se vztahují na každý typ klienta (pokračování)

Název a atributy oddílu `mqclient.ini`	**Popis**	**C a nespravováno .NET**	**Java**	**JMS**	**Spravované. NET**	**Spravované XMS .NET**
ClntSndBuffSize	Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.	Ano	Ano	Ano	Ano	Ano
Časový limit připojení	Počet sekund před pokusem o připojení k vypršení časového limitu soketu.	Ano	Ano	Ano	Ne	Ne
IPAddressVersion	Určuje protokol IP, který má být použit pro připojení kanálu.	Ano	Ne	Ne	Ano	Ano
KeepAlive	Zapne nebo vypne funkci KeepAlive .	Ano	Ano	Ano	Ano	Ano
Windows Library1	Pouze v systému Windows , název soketů DLL TCP/IP.	Ano	Ne	Ne	Ne	Ne

Multi Sekce CHANNELS konfiguračního souboru klienta

Použijte sekci CHANNELS k uvedení informací o kanálech klienta.

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

Následující atributy lze zahrnout do sekce CHANNELS:

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 UNIX Na systémech UNIX and Linux je výchozí hodnota `/var/mqm`.

ChannelDefinitionAdresář může obsahovat adresu URL, která pracuje v kombinaci s atributem ChannelDefinitionSoubor (viz “Přístup URL k tabulce CCDT” na stránce 51).

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.

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

Pokud se klientský program připojí pomocí `MQCONN`nebo nastaví volbu `MQCNO_RECONNECT_AS_DEF` pomocí `MQCONNX`, hodnota opětovného připojení nastavená pomocí DefRecon se projeví. Není-li v programu nastavena žádná hodnota opětovného připojení nebo volba DefRecon , klientský program se automaticky znovu nepřipojí.

No
Pokud není přepsáno **MQCONNX**, klient není automaticky znovu připojen.

Ano
Pokud není přepsáno **MQCONNX**, klient se automaticky znovu připojí.

QMGR
Není-li přepsáno **MQCONNX**, klient se znovu připojí automaticky, ale pouze ke stejnému správci front. Volba QMGR má stejný účinek jako MQCNO_RECONNECT_Q_MGR.

VYPNUTO
Připojení je zakázáno, a to i v případě, že o to klientský program požádá prostřednictvím volání **MQCONNX** MQI.

Automatické opětovné připojení klienta závisí na dvou hodnotách:

- Volba opětovného připojení nastavená v aplikaci
- DefRecon hodnota v souboru `mqclient.ini`

Tabulka 16. Automatické opětovné připojení závisí na hodnotách nastavených v aplikaci a v souboru mqclient.ini .

Hodnota DefRecon v `mqclient.ini`	**Volby opětovného připojení nastavené v aplikaci**			
	MQCNO_RECONNECT	MQCNO_RECONNECT_Q_MGR	MQCNO_RECONNECT_AS_DEF	MQCNO_RECONNECT_DISABLED
No	YES	QMGR	NO	NO
Ano	YES	QMGR	YES	NO
QMGR	YES	QMGR	QMGR	NO
VYPNUTO	NO	NO	NO	NO

MQReconnectTimeout
Časový limit v sekundách pro opětovné připojení ke klientovi. 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 má být použita.

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|vždy|volitelné
Produkt IBM MQ 8.0umožňuje nastavit chráněná hesla ve struktuře MQCSP namísto použití protokolu 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 naleznete v tématu Ochrana heslem MQCSP .

Související úlohy
Připojení aplikací MQI IBM MQ ke správcům front

Multi stanza cesty ClientExitkonfiguračního souboru klienta

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

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

Následující atributy mohou být zahrnuty do stanzy ClientExitPath:

ExitsDefaultCesta = *string*
Určuje umístění 32bitových kanálů kanálů pro klienty.

Tento atribut lze číst z klientů C, nespravovaných .NET, spravovaných .NET, spravovaných klientů 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 produktu Java.

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

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

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

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

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

V 9.1.2 Multi Sekce připojení konfiguračního souboru klienta

Použijte sekci připojení k uvedení názvu aplikace.

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

Následující atribut může být zahrnut do stanzy připojení:

ApplName = **`ExampleApplname`**
V konfiguračním souboru klienta můžete zadat název aplikace.

Tento atribut může používat C a nespravovaných klientů .NET .

Multi stanza JMQI konfiguračního souboru klienta

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

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

Následující atribut může být zahrnut do stanzy JMQI:

useMQCSPauthentication = **`NO|YES`**
Řídí, zda aplikace IBM MQ classes for Java a IBM MQ classes for JMS mají při ověřování u správce front používat režim kompatibility nebo režim ověřování MQCSP.

Tento atribut lze číst klienty IBM MQ classes for Javaa IBM MQ classes for JMS .

Tento atribut může mít následující hodnoty:

NO
Při ověřování u správce front použijte režim kompatibility. Toto je výchozí hodnota.

YES
Při ověřování u správce front použít režim ověřování MQCSP.

Další informace o režimu kompatibility a režimu ověření MQCSP naleznete v tématu Ověření připojení pomocí klienta Java.

Windows 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 stanza MessageBuffer konfiguračního souboru klienta

Použijte sekci MessageBuffer k uvedení informací o vyrovnávacích pamětech zpráv.

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

Do sekce MessageBuffer mohou být zahrnuty následující atributy:

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

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

Existují následující speciální hodnoty:

-1
Klient určí příslušnou hodnotu.

0
Čtení napřed je zakázáno pro klienta.

PurgeTime = *celé_číslo*|600
Interval, v sekundách, po jehož uplynutí jsou vyprázdněny zprávy ponechané ve vyrovnávací paměti dopředného čtení.

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

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

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

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

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

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

Prahová hodnota T se vypočítá takto:

```
T = Upper - Lower
```

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

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

```
Lower = Upper x UpdatePercentage / 100
```

Příklad 1:

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

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

Použití výpočtu

```
T = Upper - Lower
```

T je (100-20) = 80 Kb.

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

Příklad 2:

Atributy MaximumSize mají výchozí hodnotu 100 Kb a hodnota 40 je vybrána pro hodnotu UpdatePercentage.

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

Použití výpočtu

```
T = Upper - Lower
```

T je (100-40) = 60 kB

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

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

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

Multi stanza PreConnect konfiguračního souboru klienta

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

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

Do sekce PreConnect mohou být zahrnuty následující atributy:

Data = *uživatelská_data*

Tento atribut určuje uživatelská data, která jsou předána uživatelské proceduře pro předběžné připojení. Data předaná k proceduře předběžného připojení jsou specifická pro implementaci ukončovacího bodu před připojením, který používáte a jaká data očekává, že budou předány.

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

Tento atribut může být například použit k určení adresy URL úložiště, kde jsou uloženy definice připojení, jako 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 výstupní kód PreConnect .

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

Definice funkce dodržuje prototyp uživatelské procedury PreConnect MQ_PRECONNECT_EXIT.

Maximální délka tohoto pole je MQ_EXIT_NAME_LENGTH.

Modul = *myMod*
Název modulu obsahujícího kód ukončení rozhraní API.

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

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

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

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

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

Související úlohy
Odkazování na definice připojení pomocí předání před připojením z úložiště

Multi Sekce zabezpečení konfiguračního souboru klienta

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

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

Následující atribut může být zahrnut ve stanze zabezpečení:

DisableClientAMS = NO|YES
Atribut DisableClientAMS vám umožňuje zakázat IBM MQ Advanced Message Security (AMS), pokud používáte klienta IBM WebSphere MQ 7.5 nebo novější pro připojení ke správci front ze starší verze produktu a je hlášena chyba `2085 (MQRC_UNKNOWN_OBJECT_NAME)` .

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

Následující příklady ukazují, jak použít atribut DisableClientAMS :

- Chcete-li zakázat AMS:

```
Security:
DisableClientAMS=Yes
```

- Chcete-li povolit AMS:

```
Security:
DisableClientAMS=No
```

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

Související úlohy
Zakázání rozšířeného zabezpečení zpráv na straně klienta

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:

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 a nespravovaní klienti .NET .

ULW V 9.1.4 **AllowTLSV13 =Y | YES | T | TRUE| 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 specifikace 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 `mqclient.ini` 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 se rozhodnout zadat záznamy 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:

ŽÁDNÉ
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.

ULW V 9.1.4 **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.

ULW V 9.1.5 **OCSPTimeout = *číslo***
Počet sekund čekání na odpovídací modul OCSP 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 30 sekund.

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 sady 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.

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

Linux UNIX Při zadávání různých komponent řetězce musíte změnit význam znaků středníku pomocí zpětného lomítka, protože znak středníku je považován za komentář. Například: `'\;'`

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 být používán sadou GSKit 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 .

Solaris AIX Pro platformu Sun Solaris SPARC a 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, pokud například brána firewall zabraňuje přístupu k URL odpovídacího modulu OCSP.

ULW V 9.1.5 **SSLHTTPConnectTimeout = *číslo*|0**
Počet sekund, po které se má čekat 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*
Umístění úložiště klíčů, které obsahuje digitální certifikát uživatele, v kmenovém formátu. To znamená, že obsahuje úplnou cestu a název souboru bez přípony.

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

stanzu TCP použijte k uvedení konfiguračních parametrů síťového protokolu TCP.

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

Následující atributy mohou být zahrnuty do stanzy TCP:

ClntRcvBuffSize = *číslo*|0
Velikost vyrovnávací paměti pro příjem TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.

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

Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, a to na rozdíl od velikosti vyrovnávací paměti, které jsou opraveny produktem IBM MQ. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

ClntSndBuffSize = *číslo*|0
Velikost vyrovnávací paměti pro odeslání protokolu TCP/IP v bajtech použitá klientem kanálu připojení serveru připojení klienta na straně klienta.

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

Hodnota nula označuje, že operační systém bude spravovat velikosti vyrovnávací paměti, a to na rozdíl od velikosti vyrovnávací paměti, které jsou opraveny produktem IBM MQ. Je-li hodnota nastavena jako nula, použijí se výchozí hodnoty operačního systému. Není-li nastavena žádná hodnota, použije se standardní hodnota IBM MQ 32768.

Connect_Timeout = *číslo*
Počet sekund před pokusem o připojení k vypršení časového limitu soketu. Výchozí hodnota nula určuje, že časový limit připojení neexistuje.

Tento atribut může číst klienti C, nespravovaný .NET, IBM MQ classes for Javaa IBM MQ classes for JMS .

Proces kanálu produktu IBM MQ se připojuje přes neblokující sokety. Proto, pokud není druhý konec soketu připraven, funkce connect () se vrátí okamžitě s hodnotou *EINPROGRESS* nebo *EWOULDBLOCK*. Po této operaci bude pokus o připojení znovu proveden až do celkového počtu 20 takových pokusů, je-li hlášena chyba komunikace.

Je-li parametr Connection_Timeout nastaven na jinou hodnotu než nula, produkt IBM MQ čeká na určené časové období prostřednictvím volání select (), aby se mohl soket připravit. Tím se zvyšuje šance na úspěch následného volání connect (). Tato volba může být užitečná v situacích, kdy by připojení vyžadovalo určité čekací období kvůli vysokému zatížení na síti.

Mezi parametry Connect_Timeout, ClntSndBuffSizea ClntRcvBuffSize neexistuje žádný vztah.

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

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

Má možné řetězce hodnot `MQIPADDR_IPV4` nebo `MQIPADDR_IPV6`. Tyto hodnoty mají stejný význam jako `IPV4` a `IPV6` v **`ALTER QMGR IPADDRV`**.

KeepAlive = ANO|NE
Vypněte funkci KeepAlive zapnutou nebo vypnutou. KeepAlive=ANO způsobí, že TCP/IP pravidelně kontroluje, zda je druhý konec připojení stále dostupný. Není-li tomu tak, kanál je uzavřen.

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

Windows **Library1 = *DLLName*|WSOCK32**
(pouze Windows) Název knihovny DLL soketů TCP/IP.

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

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

V systémech UNIX and Linux a IBM i se soubor `mqat.ini` nachází v datovém adresáři správce front, což je stejné umístění jako soubor `qm.ini` .

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.

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`, `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`.

Související úlohy
Konfigurace chování trasování aktivity pomocí příkazu mqat.ini

Konfigurace distribuovaných front

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Než začnete

Před čtením této sekce je užitečné porozumět kanálům, frontám a dalším konceptům představeným v tématu Distribuované fronty a klastry.

Potřebujete-li spojit dva správce front, kteří se nacházejí v různých fyzických sítích, nebo potřebujete komunikovat přes bránu firewall, může použití produktu IBM MQ Internet Pass-Thru zjednodušit konfiguraci. Další informace naleznete v tématu IBM MQ Internet Pass-Thru.

Procedura

- K připojení aplikací pomocí distribuovaných front použijte informace z následujících dílčích témat:
  - “IBM MQ technologie distribuovaných front” na stránce 172
  - “Úvod do distribuované správy front” na stránce 190
  - “Jak odeslat zprávu jinému správci front” na stránce 193
  - “Spouštěcí kanály” na stránce 213
  - “Bezpečnost zpráv” na stránce 211
  - ULW “Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 220
  - IBM i “Monitorování a řízení kanálů v systému IBM i” na stránce 244

Související pojmy
“nastaveníIBM MQ for z/OS” na stránce 800
Toto téma můžete použít jako vodítko pro přizpůsobení vašeho 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 správce front” na stránce 265

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 81
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 795
Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 871
Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

IBM MQ technologie distribuovaných front

Dílčí témata v tomto oddílu popisují techniky, které se používají při plánování kanálů. Tato dílčí témata popisují techniky, které vám pomohou naplánovat vzájemné propojení správců front a správu toku zpráv mezi vašimi aplikacemi.

Příklady plánování kanálů zpráv viz:

- ULW Příklad plánování kanálů zpráv pro produkt UNIX, Linux, and Windows
- IBM i Příklad plánování kanálů zpráv pro produkt IBM i
- z/OS Příklad plánování kanálů zpráv pro produkt z/OS
- z/OS Příklad plánování kanálů zpráv pro produkt z/OS s použitím skupin sdílení front

Související pojmy

Kanály

Úvod do systému front zpráv

Distribuované fronty a klastry

Související úlohy

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související odkazy

Příklad konfiguračních informací

řízení toku zpráv

Řízení toku zpráv je úloha, která zahrnuje nastavení a údržbu tras zpráv mezi správci front. Je důležité pro přenosové cesty, které multi-hop přes mnoho správců front. Tento oddíl popisuje použití front, definic alias front a kanálů zpráv ve vašem systému za účelem dosažení řízení toku zpráv.

Tok zpráv řídíte pomocí mnoha technik, které byly zavedeny v produktu “Konfigurace distribuovaných front” na stránce 171. Je-li správce front v klastru, je tok zpráv řízen pomocí různých technik, jak je popsáno v tématu “řízení toku zpráv” na stránce 172. z/OS Pokud jsou správci front ve skupině sdílení front a je povoleno ukládání do front v rámci skupiny (IGQ), může být tok zpráv řízen agenty IGQ. Tito agenti jsou popsány v tématu Řazení do front v rámci skupiny.

K dosažení řízení toku zpráv můžete použít následující objekty:

- Přenosové fronty
- Kanály zpráv
- Definice vzdálené fronty
- Definice aliasu správce front

- Definice alias fronty pro odpověď

Objekty správce front a fronty jsou popsány v části Typy objektů. Kanály zpráv jsou popsány v tématu Distribuované komponenty řazení do fronty. Následující techniky používají tyto objekty k vytvoření toků zpráv ve vašem systému:

- Vložení zpráv do vzdálených front
- Směrování podle konkrétních přenosových front
- Příjem zpráv
- Předání zpráv prostřednictvím systému
- Oddělování toků zpráv
- Přepnutí toku zpráv do jiného cíle
- Vyřešení názvu fronty pro odpověď na název aliasu

Poznámka

Všechny koncepce popsané v této sekci jsou relevantní pro všechny uzly v síti a zahrnují odesílání a příjem konců kanálů zpráv. Z tohoto důvodu je ve většině příkladů ilustrován pouze jeden uzel. Výjimka je v tom případě, že příklad vyžaduje explicitní spolupráci administrátora na druhém konci kanálu zpráv.

Dříve než budete pokračovat s jednotlivými technikami, je užitečné se znovu okapovat o konceptech rozlišení názvu a o třech způsobech použití definic vzdálených front. Viz téma Distribuované fronty a klastry.

Související pojmy

“Názvy front v záhlaví přenosu” na stránce 173
Názvy cílových front cestují se zprávou v záhlaví přenosu, dokud není dosažena cílová fronta.

“Jak vytvořit správce front a odpovědět na aliasy” na stránce 173
Toto téma vysvětluje tři způsoby, jak můžete vytvořit definici vzdálené fronty.

Názvy front v záhlaví přenosu

Názvy cílových front cestují se zprávou v záhlaví přenosu, dokud není dosažena cílová fronta.

Název fronty použitý aplikací, název logické fronty, je vyřešen správcem front do názvu cílové fronty. Jinými slovy, název fyzické fronty. Tento název cílové fronty se pohybuje se zprávou v samostatné datové oblasti, záhlaví přenosu, dokud není dosaženo cílové fronty. Hlavička přenosu je poté odstraněna.

Když vytváříte paralelní třídy služeb, změníte část správce front tohoto názvu fronty. Nezapomeňte vrátit název správce front k původnímu názvu, až bude dosaženo konce přesměrování třída-služby.

Jak vytvořit správce front a odpovědět na aliasy

Toto téma vysvětluje tři způsoby, jak můžete vytvořit definici vzdálené fronty.

Objekt definice vzdálené fronty se používá třemi různými způsoby. Část Tabulka 17 na stránce 174 vysvětluje, jak definovat každý ze tří způsobů:

- Použití definice vzdálené fronty k redefinování názvu lokální fronty.

  Aplikace poskytuje při otevírání fronty pouze název fronty a tento název fronty je názvem definice vzdálené fronty.

  Definice vzdálené fronty obsahuje názvy cílové fronty a správce front. Volitelně může definice obsahovat název přenosové fronty, která má být použita. Není-li zadán žádný název přenosové fronty, správce front použije název správce front, převzaté z definice vzdálené fronty, pro název přenosové fronty. Není-li definována přenosová fronta s tímto názvem, ale je definována výchozí přenosová fronta, použije se výchozí přenosová fronta.
- Použití definice vzdálené fronty k předefinování názvu správce front.

Aplikační program nebo program kanálu poskytuje při otevření fronty název fronty spolu s názvem vzdáleného správce front.

Pokud jste zadali definici vzdálené fronty se stejným názvem jako název správce front a vy jste v definici ponechal název fronty, nahradí správce front název správce front v otevřeném volání s názvem správce front v definici.

Kromě toho může definice obsahovat název přenosové fronty, která má být použita. Není-li zadán žádný název přenosové fronty, správce front vezme název správce front, převzato z definice vzdálené fronty, pro název přenosové fronty. Není-li definována přenosová fronta s tímto názvem, ale je definována výchozí přenosová fronta, použije se výchozí přenosová fronta.

- Použití definice vzdálené fronty k redefinování názvu fronty pro odpověď.

  Pokaždé, když aplikace vloží zprávu do fronty, může poskytnout název fronty pro odpověď na zprávy odpovědi, ale s prázdnou hodnotou názvu správce front.

  Zadáte-li definici vzdálené fronty se stejným názvem jako fronta pro odpověď, nahradí lokální správce front název fronty pro odpověď s názvem fronty z vaší definice.

  V definici můžete zadat název správce front, nikoli však název přenosové fronty.

Tabulka 17. Tři způsoby použití objektu definice vzdálené fronty

Použití	**Název správce front**	**Název fronty**	**Jméno přenosové fronty**
1. Definice vzdálené fronty (při volání OPEN)			
Dodáno v rámci volání	prázdné nebo lokální QM	(*) vyžadováno	nelze použít
Dodáno v definici	povinné	povinné	volitelné
2. Alias správce front (při volání OPEN)			
Dodáno v rámci volání	(*) požadováno a nikoli lokální QM	povinné	nelze použít
Dodáno v definici	povinné	prázdná	volitelné
3. Alias fronty pro odpověď (ve volání PUT)			
Dodáno v rámci volání	prázdná	(*) vyžadováno	nelze použít
Dodáno v definici	volitelné	volitelné	prázdná

Poznámka: (*) znamená, že tento název je název objektu definice

Formální popis naleznete v tématu Rozpoznání názvu fronty.

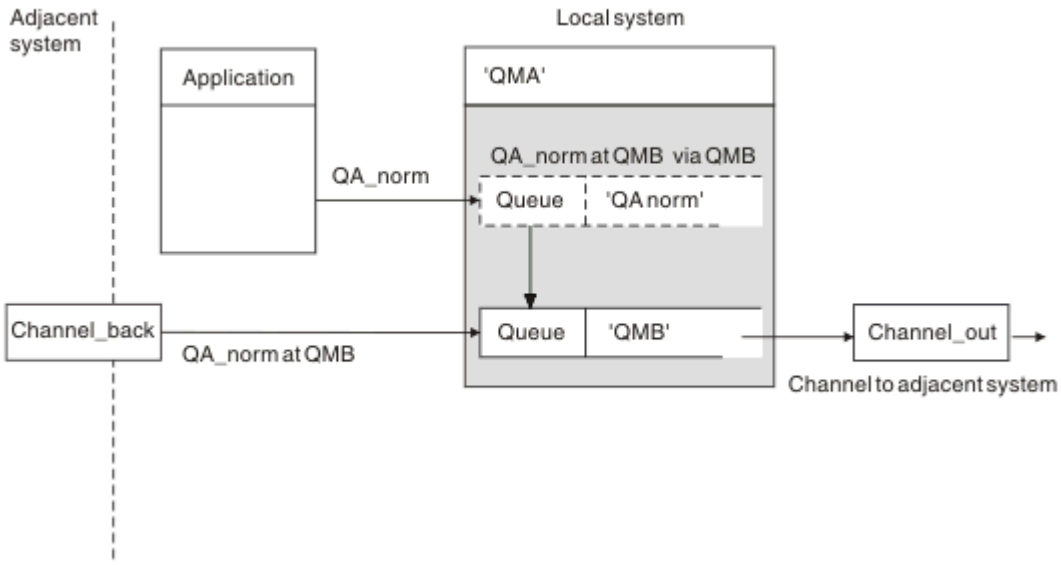
Vložení zpráv do vzdálených front

K převodu názvu fronty do přenosové fronty na sousední správce front můžete použít objekty definice vzdálené fronty.

V prostředí s distribuovanými frontami je přenosová fronta a kanál ústředním bodem pro všechny zprávy v umístění, odkud zprávy pocházejí z aplikací ve vašem lokálním systému, nebo přicházejí přes kanály ze sousedního systému. Obrázek 8 na stránce 175 zobrazuje aplikaci umístění zpráv do logické fronty s názvem 'QA_norm'. Rozpoznání názvu používá definici vzdálené fronty 'QA_norm' k výběru přenosové fronty QMB. Pak přidá záhlaví přenosu do zpráv, které uvádí 'QA_norm at QMB'.

Zprávy přicházející ze sousedního systému v systému 'Channel_back' mají záhlaví přenosu s názvem fyzické fronty 'QA_norm at QMB', například. Tyto zprávy jsou nezměněny na přenosové frontě QMB.

Kanál přesune zprávy do sousedního správce front.



Obrázek 8. Definice vzdálené fronty se používá k převedení názvu fronty na přenosovou frontu do sousedního správce front.

Jste-li administrátorem systému IBM MQ , musíte:

- Definovat kanál zpráv ze sousedního systému
- Definovat kanál zpráv na sousedící systém
- Vytvoření fronty přenosových front QMB
- Definujte objekt vzdálené fronty 'QA_norm', abyste vyřešili název fronty použité aplikacemi s názvem cílové fronty, názvem správce cílové fronty a názvem přenosové fronty.

V prostředí klastrování je třeba definovat pouze kanál příjemce klastru v lokálním správci front. Frontu přenosu nebo objekt vzdálené fronty není třeba definovat. Viz Klastry.

Další informace o rozlišování názvů

Efekt definice vzdálené fronty je definovat název fyzické cílové fronty a název správce front. Tyto názvy jsou vloženy do záhlaví přenosu zpráv.

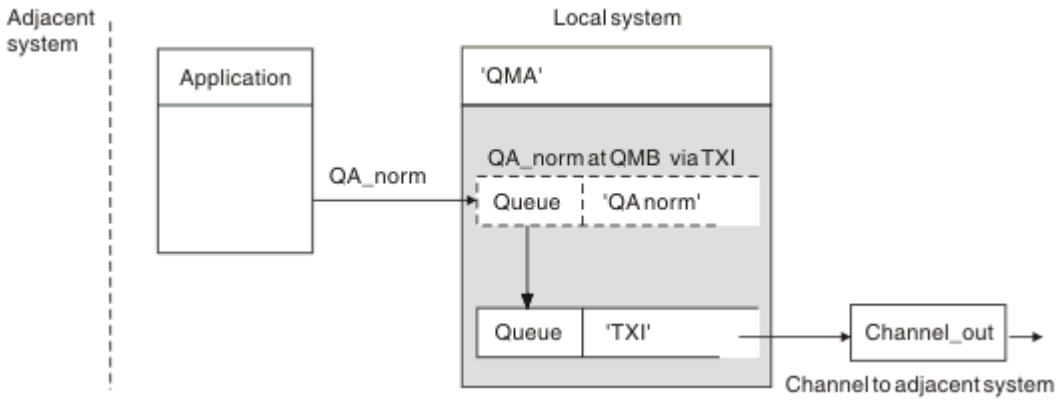
Příchozí zprávy ze sousedního systému již mají tento typ rozpoznání názvu, který provedl původní správce front. Proto mají záhlaví přenosu zobrazující název fyzické cílové fronty a název správce front. Tyto zprávy nejsou ovlivněny definicemi vzdálených front.

Související odkazy

Rozlišení názvu fronty

Výběr přenosové fronty

Chcete-li povolit odesílání zpráv stejnému sousednímu správci front, můžete použít definici vzdálené fronty k tomu, abyste povolili odesílání zpráv jinou přenosovou frontu.



Obrázek 9. Definice vzdálené fronty umožňuje použití jiné přenosové fronty.

Když v prostředí rozděleném do front potřebujete změnit tok zpráv z jednoho kanálu na druhý, použijte stejnou konfiguraci systému, jak je zobrazeno v Obrázek 8 na stránce 175 v “Vložení zpráv do vzdálených front” na stránce 174. Obrázek 9 na stránce 176 v tomto tématu ukazuje, jak používat definici vzdálené fronty k odesílání zpráv přes jinou přenosovou frontu, a tím i přes jiný kanál, do stejného sousedního správce front.

Pro konfiguraci zobrazenou v Obrázek 9 na stránce 176musíte poskytnout objekt vzdálené fronty 'QA_norm' a přenosovou frontu 'TX1'. Musíte zadat 'QA_norm', abyste vybrali frontu 'QA_norm' ve vzdáleném správci front, přenosové frontě 'TX1' a správce front 'QMB_priority'. Určete 'TX1' v definici kanálu sousedící se systémem.

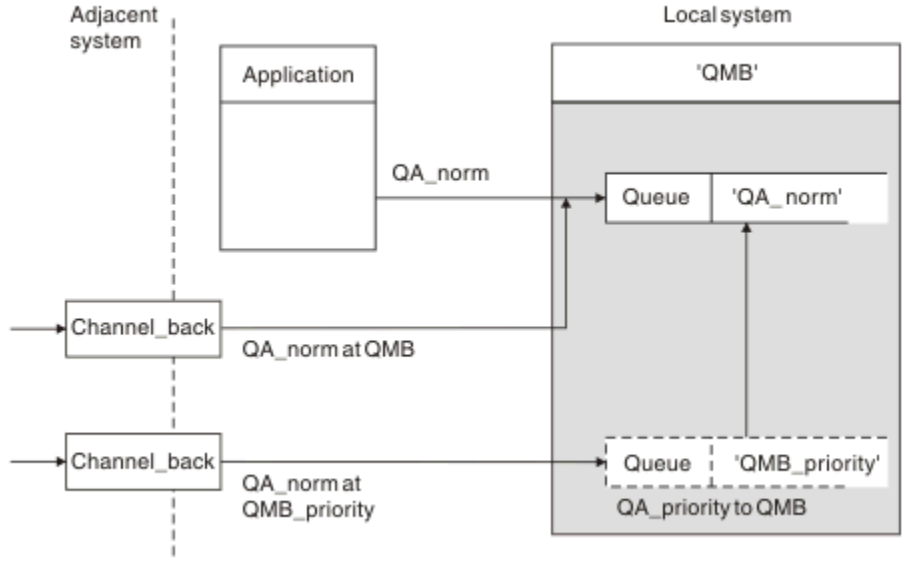
Zprávy jsou umístěny do přenosové fronty 'TX1' s hlavičkou přenosu obsahujícím 'QA_norm při QMB_priority' a jsou posílána přes kanál na sousední systém.

Seznam kanálů byl z tohoto obrázku odstraněn, protože by potřeboval alias správce front.

V klastrovaném prostředí není třeba definovat přenosovou frontu nebo definici vzdálené fronty. Další informace viz “Definování front klastru” na stránce 266.

Příjem zpráv

Správce front je možné nakonfigurovat tak, aby přijímal zprávy od jiných správců front. Je třeba zajistit, aby nedošlo k neúmyslnému rozpoznání názvu.



Obrázek 10. Přímé přijímání zpráv a řešení názvu správce front aliasu

Stejně jako uspořádání zpráv, které mají být odeslány, musí správce systému také zajistit, aby zprávy byly přijaty ze sousedních správců front. Přijaté zprávy obsahují fyzický název cílového správce front a fronty v záhlaví přenosu. Jsou s nimi stejné jako zprávy z lokální aplikace určující název správce front i název fronty. Kvůli této léčbě byste měli zajistit, aby zprávy vstupující do vašeho systému neměly nezáměrné rozlišení jména provedeno. Tento scénář viz Obrázek 10 na stránce 176 .

Pro tuto konfiguraci musíte připravit:

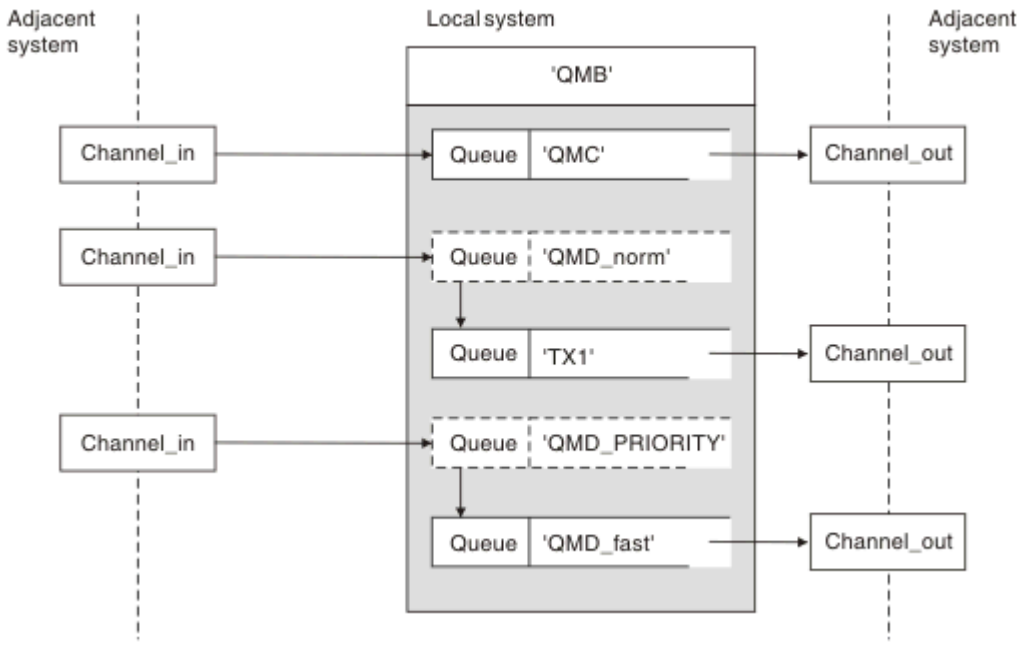
- Kanály zpráv pro příjem zpráv ze sousedních správců front
- Definice aliasu správce front k vyřešení příchozího toku zpráv, 'QMB_priority', do lokálního názvu správce front, 'QMB'
- Lokální fronta, 'QA_norm', pokud neexistuje,

Přijímání názvů správce front aliasu

Použití definice aliasu správce front v této ilustraci nevedlo k výběru jiného cílového správce front. Zprávy, které prošly tímto lokálním správcem front a adresované na 'QMB_priority', jsou určeny pro správce front 'QMB'. Název správce alias fronty se používá k vytvoření samostatného toku zpráv.

Předání zpráv prostřednictvím systému

Zprávy můžete předávat prostřednictvím systému třemi způsoby-pomocí názvu umístění, s použitím aliasu pro správce front nebo výběrem přenosové fronty.



Obrázek 11. Tři metody posílání zpráv přes váš systém

Technika zobrazená v Obrázek 10 na stránce 176 v “Příjem zpráv” na stránce 176ukázala, jak je zachycen tok alias. Obrázek 11 na stránce 177 ilustruje, jak jsou sítě vybudovány tím, že dohromady techniky popsané dříve.

Konfigurace zobrazuje kanál doručující tři zprávy s různými místy určení:

1. QB rovno QMC
2. QB rovno QMD_norm
3. QB rovno QMD_PRIORITY

První tok zpráv musíte přenést prostřednictvím systému nezměněný. Druhý tok zpráv je třeba předat prostřednictvím jiné přenosové fronty a kanálu. Pro druhý tok zpráv je třeba také vyřešit zprávy pro název aliasu správce front `QMD_norm` správci front `QMD`. Třetí tok zpráv zvolí jinou přenosovou frontu bez jakékoli jiné změny.

V klastrovém prostředí jsou zprávy předávány prostřednictvím přenosové fronty klastru. Za normálních okolností jedna přenosová fronta `SYSTEM.CLUSTER.TRANSMIT.QUEUE`přenáší všechny zprávy do všech správců front ve všech klastrech, jejichž členem je správce front; viz Klastr správců front. Můžete definovat samostatné přenosové fronty pro všechny správce front nebo některé z nich v klastrech, jejichž členem je správce front.

Následující metody popisují metody použitelné pro prostředí s distribuovaným řazením do fronty.

Použít tyto metody

Pro tyto konfigurace musíte připravit:

- Definice vstupního kanálu
- Definice výstupního kanálu
- Přenosové fronty:
  - `QMC`
  - `TX1`
  - `QMD_fast`
- Definice aliasů správce front:
  - `QMD_norm` with `QMD_norm` to `QMD` through `TX1`
  - `QMD_PRIORITY` with `QMD_PRIORITY` to `QMD_PRIORITY` through `QMD_fast`

Poznámka: Žádná z toků zpráv zobrazených v příkladu nemění cílovou frontu. Alias názvu správce front poskytuje oddělení toků zpráv.

Metoda 1: Použít název příchozího umístění

Obdržíte zprávy s hlavičkou přenosu, která obsahuje jiné jméno umístění, jako např. `QMC`. Nejjednodušší konfigurací je vytvořit přenosovou frontu s tímto názvem, `QMC`. Kanál, který obsluhuje přenosovou frontu, předá zprávu nezměněnou na další místo určení.

Metoda 2: Použít alias pro správce front

Druhá metoda je použití definice alias objektu správce front, ale zadejte nový název umístění, `QMD`a konkrétní přenosovou frontu, `TX1`. Tato akce:

- Ukončuje tok zpráv aliasu nastavený aliasem názvu správce front `QMD_norm`, tj. jmenovanou třídou služby `QMD_norm`.
- Změní záhlaví přenosu na těchto zprávách z `QMD_norm` na `QMD`.

Metoda 3: Vyberte přenosovou frontu

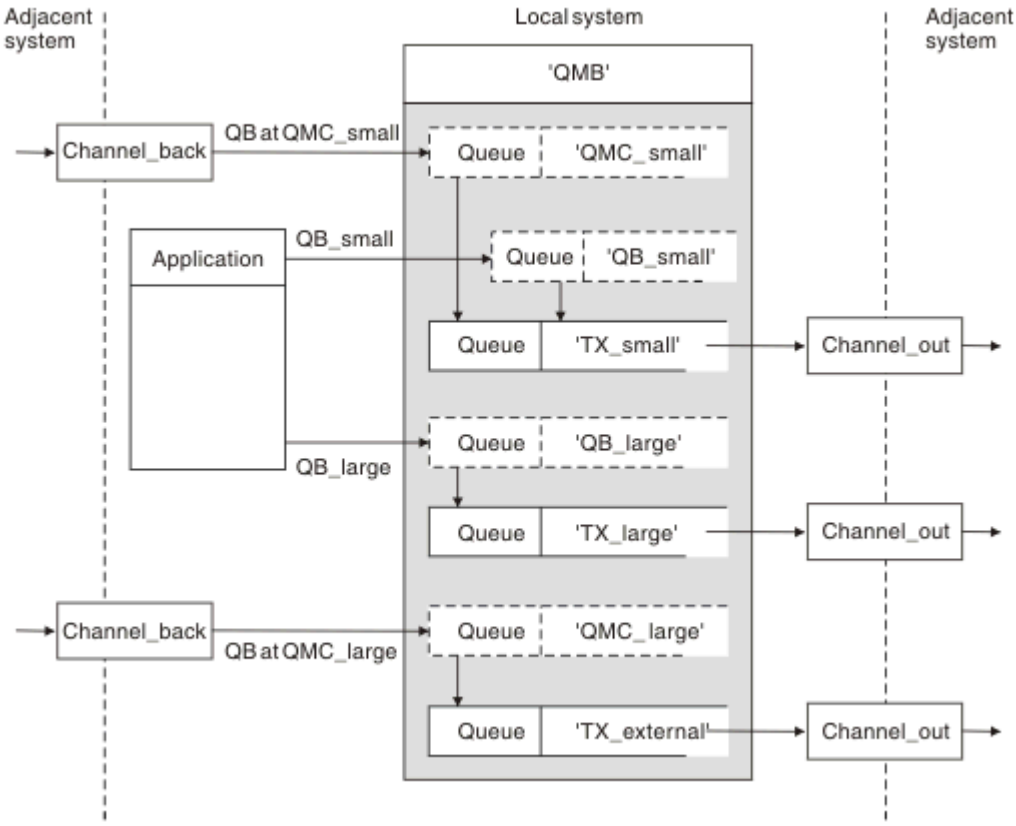
Třetí metodou je alias objektu správce front definovaný se stejným názvem jako cílové umístění, `QMD_PRIORITY`. Definice aliasu správce front slouží k výběru konkrétní přenosové fronty, produktu `QMD_fast`, a tedy jiného kanálu. Hlavičky přenosu na těchto zprávách zůstanou nezměněny.

Oddělování toků zpráv

Alias správce front můžete použít k vytvoření samostatných toků zpráv k odesílání zpráv do stejného správce front.

V prostředí s distribuovaným řazením může dojít k různým příčinám, že je třeba oddělit zprávy od stejného správce front do různých toků zpráv. Příklad:

- Je možné, že budete potřebovat samostatný tok pro velké, střední a malé zprávy. Tato potřeba se také používá v klastrovém prostředí, a v tomto případě můžete vytvářet klastry, které se překrývají. Existuje mnoho důvodů, proč byste tak mohli učinit, například:
  - Chcete-li umožnit různým organizacím, aby měly vlastní administraci.
  - Umožněte administraci nezávislých aplikací samostatně.
  - Vytvoření třídy služeb. Předpokládejme například, že máte klastr s názvem PERSONÁL, který je podmnožinou klastru s názvem STUDENTS. Když vložíte zprávu do fronty oznámené v klastru STAFF, bude použit vyhrazený kanál. Když vložíte zprávu do fronty oznámené v klastru STUDENTS, lze použít buď obecný kanál, nebo omezený kanál.
  - Vytvoření testovacího a produkčního prostředí.
- Je možné, že bude nutné směrovat příchozí zprávy různými cestami z cesty lokálně generovaných zpráv.
- Vaše instalace může vyžadovat naplánování přesunu zpráv v určitých časech (například přes noc) a zprávy pak musí být uloženy ve vyhrazených frontách, dokud není naplánováno.



Obrázek 12. Oddělení toků zpráv

V příkladu uvedeném v souboru Obrázek 12 na stránce 179jsou dva příchozí toky alias názvů správce front 'QMC_small' a 'QMC_large'. Tyto toky jsou určeny pro zachycení těchto toků pro lokálního správce front pomocí definice alias správce front. Máte aplikaci adresující dvě vzdálené fronty a vy potřebujete tyto toky zpráv uchovávat odděleně. Poskytujete dvě definice vzdálených front, které určují stejné umístění, 'QMC', ale specifikujte různé přenosové fronty. Tato definice uchovává toky odděleně a v konečném důsledku není třeba nic dalšího, protože mají stejný cílový název správce front v záhlavích přenosu. Poskytujete:

- Definice příchozího kanálu
- Dvě definice vzdálených front QB_small a QB_large

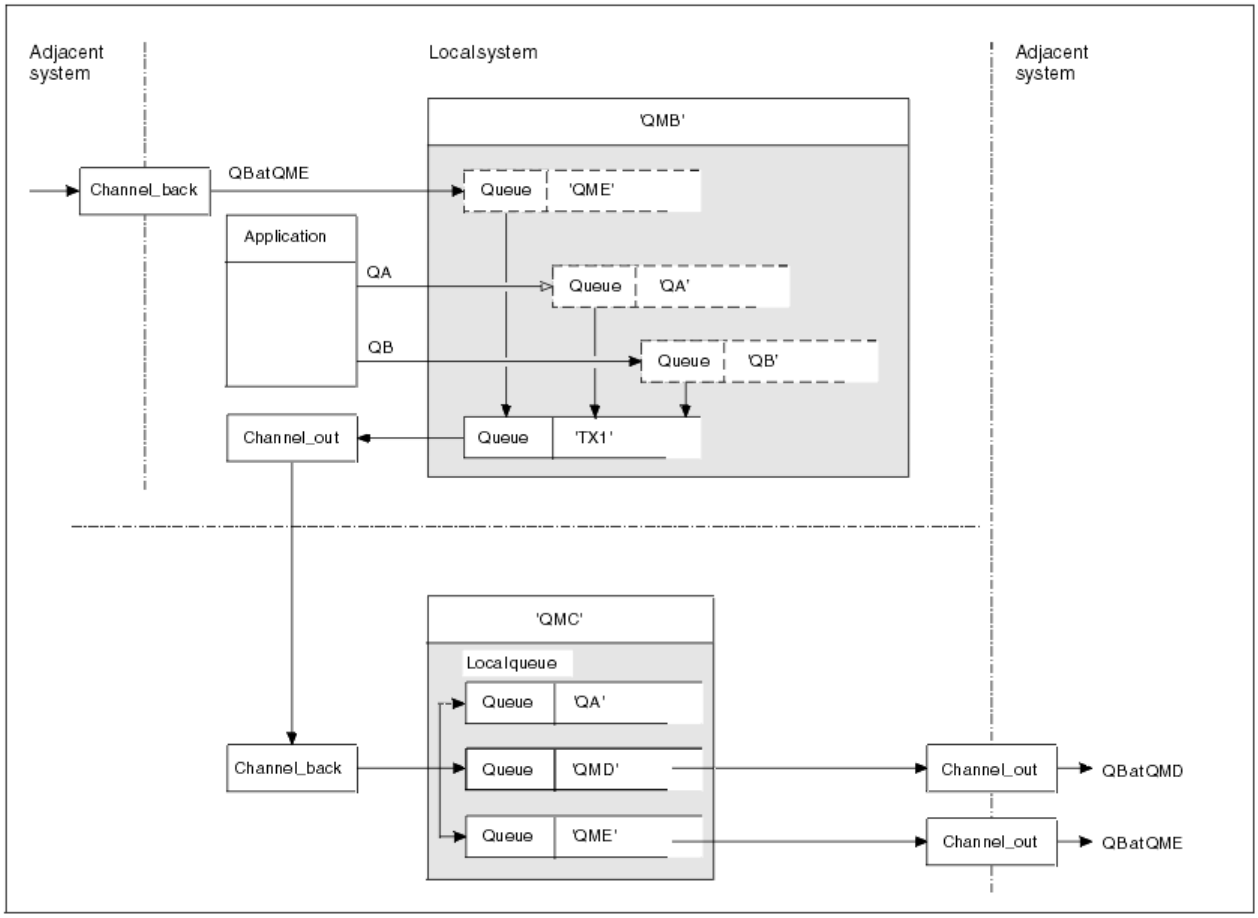
- Dva definice aliasů správce front QMC_small a QMC_large
- Tři definice odesílajícího kanálu
- Tři přenosové fronty: TX_small, TX_large, a TX_external

Koordinace se sousedními systémy

Používáte-li alias správce front k vytvoření samostatného toku zpráv, je třeba koordinovat tuto aktivitu s administrátorem systému na vzdáleném konci kanálu zpráv a zajistit tak, aby byl k dispozici odpovídající alias správce front.

Soustředění zpráv na různá místa

Můžete se soustředit na zprávy určené pro různá umístění na jednom kanálu.



Obrázek 13. Sloučení toků zpráv na kanál

Obrázek 13 na stránce 180 ilustruje techniku distribuované fronty pro soustředění zpráv, které jsou určeny pro různá umístění na jednom kanálu. Dvě možné použití by byla:

- Soustředí se na provoz zpráv prostřednictvím brány
- Použití širokých dálnic šířky pásma mezi uzly

V tomto příkladu jsou zprávy z různých zdrojů, lokální a sousední a mající různé cílové fronty a správce front odesílány prostřednictvím přenosové fronty 'TX1' ke správci front QMC správce front. Správce front QMC doručuje zprávy podle míst určení. Jedna sada do přenosové fronty 'QMD' pro další přenos do správce front QMD. Jiný je nastaven na přenosovou frontu 'QME' pro další přenos do správce front QME. Další zprávy jsou vloženy do lokální fronty 'QA'.

Musíte zadat:

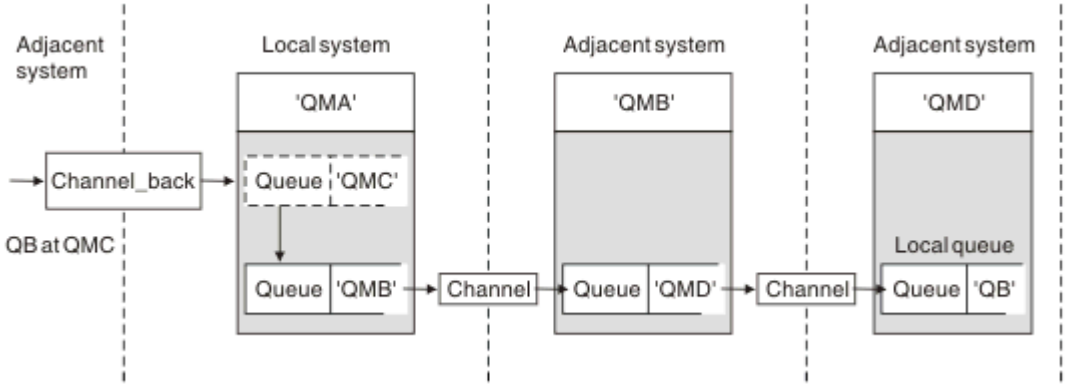
- Definice kanálů
- Přenosová fronta TX1
- Definice vzdálených front:
  - QA s QA v QMC přes TX1'
  - QB s 'QB při QMD přes TX1'
- Definice aliasu správce front:
  - QME se 'QME přes TX1'

Doplňkový administrátor, který konfiguruje QMC, musí poskytovat:

- Příjem definice kanálu se stejným názvem kanálu
- Přenosová fronta QMD s přidruženou definicí odesílajícího kanálu
- Přenosová fronta QME s přidruženou definicí odesílajícího kanálu
- Lokální objekt fronty QA.

Odklonění toku zpráv do jiného cíle

Můžete předefinovat místo určení určitých zpráv pomocí aliasů správce front a přenosových front.



Obrázek 14. Odklonění proudů zpráv do jiného cíle

Obrázek 14 na stránce 181 ilustruje, jak můžete předefinovat místo určení určitých zpráv. Příchozí zprávy pro QMA jsou určeny pro 'QB v QMC'. Běžně se dostanou do QMA a budou umístěny do přenosové fronty s názvem QMC, která byla součástí kanálu do QMC. QMA musí odklonit zprávy na QMD, ale je schopen dosáhnout pouze QMD přes QMB. Tato metoda je užitečná, když potřebujete přesunout službu z jednoho umístění do jiného a umožnit odběratelům pokračovat v odesílání zpráv dočasným způsobem, dokud se nepřizpůsobují nové adrese.

Metoda opětného mapování příchozích zpráv určených pro určitého správce front do jiného správce front:

- Alias správce front pro změnu cílového správce front na jiného správce front a výběr přenosové fronty pro sousední systém.
- Přenosová fronta, která má sloužit sousednímu správci front
- Přenosová fronta v sousedním správci front pro následné směrování do cílového správce front.

Musíte zadat:

- Definice kanálu Channel_back
- Definice alias objektu správce front QMC s QB při QMD až QMB
- Definice objektu Channel_out
- Přidružená přenosová fronta QMB

Další administrátor, který konfiguruje QMB, musí poskytovat:

- Odpovídající definice channel_back
- Přenosová fronta, QMD
- Přidružená definice kanálu pro QMD.

Aliasy lze používat v klastrovém prostředí. Informace viz “Aliasy správce front a klastry” na stránce 358.

Odesílání zpráv do rozdělovníku

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

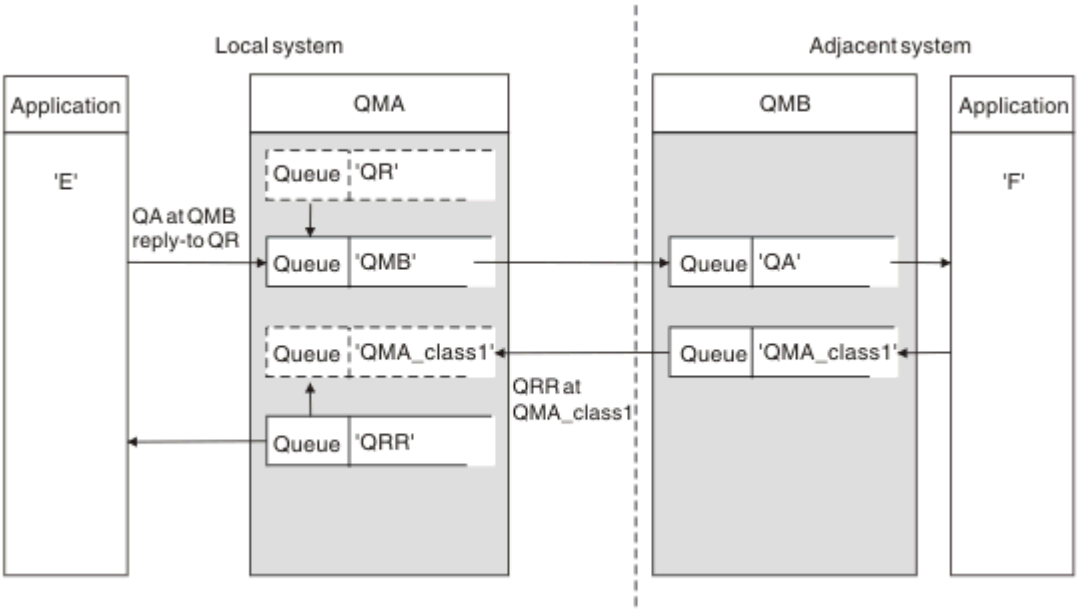
Ve IBM MQ na všech platformách kromě z/OSmůže aplikace odeslat zprávu do několika cílů s jedním voláním MQPUT. Můžete to provést jak v prostředí rozděleném do front, tak i v prostředí klastrů. Musíte definovat cíle v rozdělovníku, jak je popsáno v tématu Distribuční seznamy.

Ne všichni správci front podporují distribuční seznamy. Když agent MCA naváže spojení s partnerem, určí, zda partner podporuje rozdělovníky a nastaví příznak přenosové fronty na odpovídajícím způsobem. Pokud se aplikace pokusí odeslat zprávu, která je určena pro distribuční seznam, ale partner nepodporuje distribuční seznamy, odesílající agent MCA zachytí zprávu a vloží ji do přenosové fronty jednou pro každé zamýšlené místo určení.

Přijímající agent MCA zajistí, aby zprávy odeslané do distribučního seznamu byly bezpečně přijaty ve všech zamýšlených cílech. Pokud některá místa určení selžou, agent MCA zjistí, které z nich selhaly. Pak může generovat zprávy o výjimkách pro ně a může se pokusit o jejich odeslání znovu.

Fronta pro odpověď

Můžete vytvořit úplnou smyčku zpracování vzdálených front pomocí fronty pro odpovědi.



Obrázek 15. Substituce názvu fronty pro odpověď během volání PUT

V produktu Obrázek 15 na stránce 182se zobrazí úplná smyčka zpracování vzdálených front s použitím fronty pro odpověď. Tato smyčka se používá jak v prostředí s rozdělenou do front, tak i v prostředí klastrů. Podrobnosti jsou uvedeny v tématu Tabulka 21 na stránce 189.

Aplikace otevře QA na QMB a vloží zprávy do této fronty. Pro zprávy je zadán název fronty QR pro odpověď bez správce front, který je určen. Správce front QMA nalezne objekt QR s odpovědí na frontu QR a extrahuje z něj alias QRR a název správce front QMA_class1. Tyto názvy jsou vloženy do polí pro odpověď na zprávy.

Odpovědi na zprávy z aplikací v QMB jsou adresovány na QRR na QMA_class1. Definice názvu aliasu správce front QMA_class1 je používána správcem front k toku zpráv do sebe sama a do fronty QRR.

Tento scénář popisuje způsob, jakým aplikacím poskytujete službu pro výběr třídy služeb pro zprávy odpovědí. Třída je implementována přenosovou frontou QMA_class1 v QMB, spolu s definicí aliasu správce front QMA_class1 na QMA. Tímto způsobem můžete změnit odpověď aplikace na frontu tak, aby toky byly odděleny, aniž by bylo třeba aplikace zahrnovat. Aplikace vždy volí QR pro tuto konkrétní třídu služeb. Máte možnost změnit provozní třídu s definicí QR odpovědi na frontu pro odpověď.

Musíte vytvořit:

- QR definice odpovědi na frontu
- QMB objektu přenosové fronty
- Definice objektu Channel_out
- Definice kanálu Channel_back
- Definice aliasu správce front QMA_class1
- Objekt lokální fronty QRR, pokud neexistuje

Další administrátor v sousedním systému musí vytvořit:

- Definice přijímajícího kanálu
- Objekt přenosové fronty QMA_class1
- Přidružený odesílající kanál
- Lokální objekt fronty QA.

Vaše aplikační programy používají:

- Název fronty pro odpověď na název fronty QR při vložení volání
- Název fronty QRR pro volání get

Tímto způsobem můžete podle potřeby změnit provozní třídu, aniž by bylo nutné aplikaci používat. Změňte odpověď na alias 'QR', spolu s přenosovou frontou 'QMA_class1' a aliasem správce front 'QMA_class1'.

Není-li při vložení zprávy do fronty nalezen žádný objekt aliasu pro odpověď na alias, bude název lokálního správce front vložen do prázdného pole názvu správce front pro odpověď. Název fronty pro odpovědi zůstává nezměněn.

Omezení rozlišování názvů

Vzhledem k tomu, že při vložení původní zprávy bylo provedeno rozpoznání názvu pro frontu pro odpověď na frontu 'QMA', není povoleno žádné další rozlišení názvu v 'QMB '. Zpráva se umístí s fyzickým názvem odpovědi do fronty odpovědí aplikací.

Aplikace si musí být vědomy toho, že název, který používají pro frontu pro odpověď, se liší od názvu skutečné fronty, kde se mají vratové zprávy nalézt.

Když jsou například pro použití aplikací s aliasy fronty pro odpověď na aliasC1_alias'a'C2_alias' poskytnuty dvě třídy služeb, používají aplikace tyto názvy jako názvy front pro odpověď ve volaných volaných zprávách. However, the applications actually expect messages to appear in queues 'C1' for 'C1_alias' and 'C2' for 'C2_alias'.

Avšak aplikace je schopna provést dotazové volání na frontu alias pro odpověď, aby zkontroloval jméno skutečné fronty, kterou musí použít k získání zpráv odpovědi.

Související pojmy

“Jak vytvořit správce front a odpovědět na aliasy” na stránce 173
Toto téma vysvětluje tři způsoby, jak můžete vytvořit definici vzdálené fronty.

“Příklad alias fronty pro odpověď” na stránce 184

Tento příklad ilustruje použití aliasu odpovědi na alias pro výběr jiné přenosové cesty (přenosové fronty) pro vrácené zprávy. Použití této funkce vyžaduje, aby se název fronty pro odpověď změnil ve spolupráci s aplikacemi.

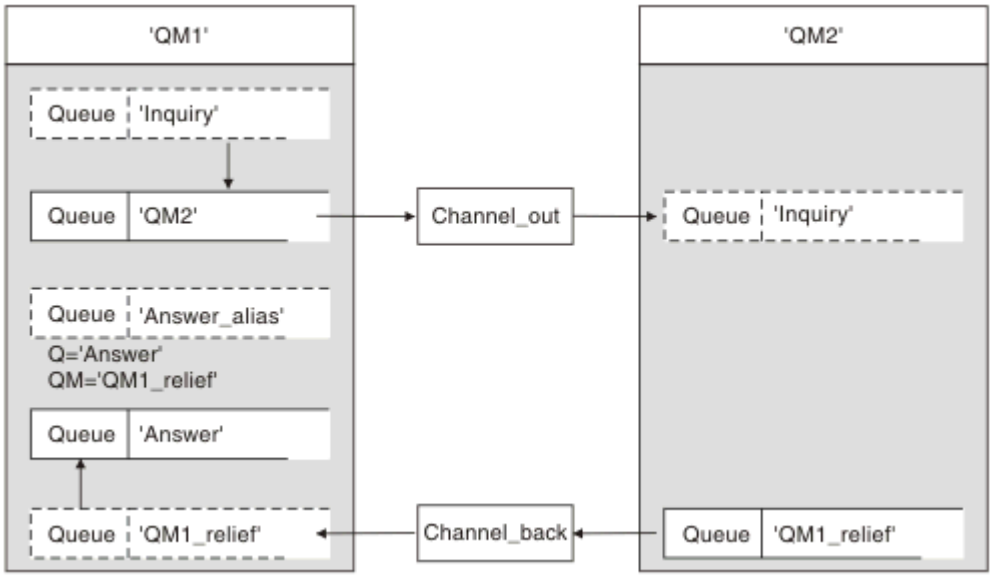
“Jak příklad funguje” na stránce 185
Vysvětlení příkladu a způsobu, jakým správce front používá alias fronty pro odpověď.

“Průchodná odpověď na alias fronty pro odpověď” na stránce 186
Průchod procesu z aplikace, který vkládá zprávu do vzdálené fronty do stejné aplikace a odebírá zprávu odpovědi z alias odpovědi alias.

Příklad alias fronty pro odpověď

Tento příklad ilustruje použití aliasu odpovědi na alias pro výběr jiné přenosové cesty (přenosové fronty) pro vrácené zprávy. Použití této funkce vyžaduje, aby se název fronty pro odpověď změnil ve spolupráci s aplikacemi.

Jak je zobrazeno v Obrázek 16 na stránce 184, zpáteční cesta musí být k dispozici pro zprávy odpovědi včetně alias přenosové fronty, kanálu a aliasu správce front.



Obrázek 16. Příklad alias fronty pro odpověď

Tento příklad je určen pro aplikace žadatele na 'QM1', které posílají zprávy do aplikací serveru na 'QM2'. Zprávy na serveru se mají vracet prostřednictvím alternativního kanálu s použitím přenosové fronty 'QM1_relief' (výchozí návratový kanál bude obsluhován s přenosovou frontou 'QM1').

Alias fronty pro odpověď je konkrétní použití definice vzdálené fronty s názvem 'Answer alias'. Aplikace v QM1 zahrnují tento název, 'Answer_alias', v poli odpovědi na všechny zprávy, které vložili do fronty 'Inquiry'.

Definice fronty odpovědí 'Answer alias' je definována jako 'Answer at QM1_relief'. Aplikace v QM1 očekávají, že se jejich odpovědi zobrazí v lokální frontě s názvem 'Answer'.

Serverové aplikace na úrovni QM2 používají pole odpovědi na přijaté zprávy k získání názvů front a správců front pro zprávy odpovědí žadateli na QM1.

Definice použité v tomto příkladu na QM1

Administrátor systému IBM MQ na QM1 musí zajistit, aby byla vytvořena odpověď na frontu 'Answer' spolu s dalšími objekty. Název aliasu správce front označený pomocí znaku '*' musí souhlasit s názvem správce front v definici alias fronty pro odpověď, který je také označen jako '*'.

Objekt	Definice	
Lokální přenosová fronta	QM2	
Definice vzdálené fronty	Název objektu	Inquiry
	Název vzdáleného správce front	QM2
	Název vzdálené fronty	Inquiry
	Jméno přenosové fronty	QM2 (DEFAULT)
Alias správce front	Název objektu	QM1_relief *
	Název správce front	QM1
	Název fronty	(prázdné)
Alias fronty pro odpověď	Název objektu	alias_odpovědi
	Název vzdáleného správce front	QM1_relief *
	Název vzdálené fronty	Přijmout

Definice vložení na QM1

Aplikace vyplňují odpověď na pole s názvem aliasu fronty odpovědí a ponechte pole názvu správce front prázdné.

Pole	Obsah
Název fronty	Inquiry
Název správce front	(prázdné)
Název fronty pro odpověď	alias_odpovědi
Správce front pro odpovědi	(prázdné)

Definice použité v tomto příkladu na QM2

Administrátor systému IBM MQ na QM2 se musí ujistit, že lokální fronta existuje pro příchozí zprávy a že správně pojmenovaná přenosová fronta je k dispozici pro zprávy odpovědi.

Objekt	Definice
Lokální fronta	Inquiry
Přenosová fronta	QM1_relief

Definice vložení na QM2

Aplikace v QM2 načtou název fronty a název správce front z původní zprávy a použijí je při vložení zprávy odpovědi do fronty pro odpověď.

Pole	Obsah
Název fronty	Přijmout
Název správce front	QM1_relief

Jak příklad funguje

Vysvětlení příkladu a způsobu, jakým správce front používá alias fronty pro odpověď.

V tomto příkladu aplikace žadatele v QM1 vždy používají 'Answer alias' jako frontu pro odpověď v příslušném poli volání příkazu put. Vždy načtou své zprávy z fronty s názvem 'Odpověď'.

Definice alias fronty pro odpověď jsou k dispozici pro použití administrátorem systému QM1 ke změně názvu odpovědi na frontu odpovědí a návratové cesty 'QM1_relief'.

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

Jak správce front používá alias fronty odpovědí na frontu

Správce front QM1 načte definice z aliasu fronty pro odpověď, je-li název fronty pro odpověď, zahrnutý v volaném volání aplikace, stejný jako alias fronty pro odpověď a část správce front je prázdná.

Správce front nahradí název fronty pro odpověď v umístění volání s názvem fronty z definice. Nahrazuje prázdný název správce front v rámci volání put s názvem správce front z definice.

Tyto názvy jsou přenášeny spolu se zprávou v deskriptoru zpráv.

Tabulka 18. Alias fronty pro odpověď

Název pole	**Volání vložení**	**Hlavička přenosu**
Název fronty pro odpověď	alias_odpovědi	Přijmout
Název správce front pro odpověď	(prázdné)	QM1_relief

Průchodná odpověď na alias fronty pro odpověď

Průchod procesu z aplikace, který vkládá zprávu do vzdálené fronty do stejné aplikace a odebírá zprávu odpovědi z alias odpovědi alias.

Chcete-li dokončit tento příklad, podívejme se na proces.

1. Aplikace otevře frontu s názvem 'Inquiry' a vloží do ní zprávy. Aplikace nastaví pole odpovědi na pole deskriptoru zprávy na:

Název fronty pro odpověď	**alias_odpovědi**
Název správce front pro odpověď	(prázdné)

2. Správce front 'QM1' odpovídá na prázdný název správce front tím, že zkontroluje definici vzdálené fronty s názvem 'Answer alias'. Není-li nalezena žádná hodnota, správce front umístí své vlastní jméno 'QM1' do pole správce front pro odpověď na deskriptor zprávy.
3. Pokud správce front nalezne definici vzdálené fronty s názvem 'Answer alias', extrahuje název fronty a názvy správce front z definice (název fronty= 'Answer' a správce front name= 'QM1_relief'). Pak je umístí do polí deskriptoru zpráv do odpovědi.
4. Správce front 'QM1' používá definici vzdálené fronty 'Inquiry', aby určil, že zamýšlená cílová fronta je ve správci front 'QM2', a zpráva se umístí do přenosové fronty 'QM2'. 'QM2' je výchozí název přenosové fronty pro zprávy určené pro fronty ve správci front 'QM2'.
5. Když správce front 'QM1' vloží zprávu do přenosové fronty, přidá do zprávy záhlaví přenosu. Toto záhlaví obsahuje název cílové fronty, 'Inquiry' a správce cílové fronty 'QM2'.
6. Zpráva dorazí do správce front 'QM2' a je umístěna v lokální frontě 'Inquiry'.
7. Aplikace získá zprávu z této fronty a zpracuje zprávu. Aplikace připraví zprávu odpovědi a vloží tuto zprávu odpovědi na název fronty pro odpovědi z deskriptoru zprávy původní zprávy:

Název fronty pro odpověď	**Přijmout**
Název správce front pro odpověď	QM1_relief

8. Správce front 'QM2' provádí příkaz put. Nalezení názvu správce frontQM1_reliefje vzdáleným správcem front, který umístí zprávu do přenosové fronty se stejným názvem, 'QM1_relief'. Zobrazí se zpráva obsahující záhlaví přenosu obsahující název cílové fronty, 'Odpověď' a správce cílové fronty 'QM1_relief'.
9. Zpráva se přenese do správce front 'QM1'. Správce front rozpozná, že název správce front 'QM1_relief' je alias, extrakty z definice aliasu 'QM1_relief', název správce fyzických front 'QM1'.

10. Správce front 'QM1' pak vloží zprávu do názvu fronty obsaženého v záhlaví přenosu, 'Answer'.
11. Aplikace extrahuje svou zprávu odpovědi z fronty 'Answer'.

Faktory související

V prostředí s distribuovaným řazením do fronty, protože cíle zpráv jsou adresovány pouze s názvem fronty a názvem správce front, platí určitá pravidla.

1. Je-li zadán název správce front a název se liší od názvu lokálního správce front, postupujte takto:
   - Přenosová fronta musí být k dispozici se stejným názvem. Tato přenosová fronta musí být součástí kanálu zpráv přesouváním zpráv do jiného správce front, nebo
   - Definice aliasu správce front musí existovat, aby bylo možné název správce front převést na stejný nebo jiný název správce front a volitelnou přenosovou frontu, nebo
   - Pokud nemůže být název přenosové fronty vyřešen a byla definována výchozí přenosová fronta, použije se výchozí přenosová fronta.
2. Je-li zadán pouze název fronty, musí být ve správci lokální fronty k dispozici fronta libovolného typu, ale se stejným názvem. Tato fronta může být definicí vzdálené fronty, která se řeší jako: přenosová fronta se sousedním správcem front, názvem správce front a volitelnou přenosovou frontou.

Informace o tom, jak to funguje v klastrovém prostředí, najdete v tématu Klastry.

z/OS Jsou-li správci front spuštění ve skupině sdílení front (QSG) a ve frontě v rámci skupiny (IGQ) je povoleno, můžete použít SYSTEM.QSG.TRANSMIT.QUEUE. Další informace naleznete v tématu Řazení do front v rámci skupiny.

Zvažte scénář přesunu zpráv kanálu zpráv z jednoho správce front do jiného v prostředí s distribuovaným řazením do fronty.

Přesunuté zprávy pocházely z libovolného jiného správce front v síti a některé zprávy mohou přicházet s neznámým názvem správce front jako cíl. K tomuto problému může dojít, když se název správce front například změnil nebo byl odebrán ze systému.

Program kanálu rozpozná tuto situaci, když nemůže najít přenosovou frontu pro tyto zprávy, a umístí zprávy do fronty nedoručených zpráv (dead-letter). Je vaší zodpovědností hledat tyto zprávy a zařídit, aby byly přesměrovány na správné místo určení. Případně je vraťte původci, kde je možné původce zjistit.

Za těchto okolností jsou generovány zprávy o výjimkách, pokud byly zprávy sestavy požadovány v původní zprávě.

Konvence rozpoznávání názvů

Rozpoznání názvu, které mění identitu cílové fronty (tj. se změnou fyzického názvu), se vyskytuje pouze jednou a pouze u původního správce front.

Následné použití různých možností aliasu musí být použito pouze při oddělování a kombinování toků zpráv.

Zpětné směrování

Zprávy mohou obsahovat návratovou adresu ve formě názvu fronty a správce front. Tento formulář návratové adresy lze použít jak v prostředí s rozdělenou do front, tak i v prostředí klastrů.

Tato adresa je obvykle určena aplikací, která vytváří zprávu. Může být upraven libovolnou aplikací, která pak tuto zprávu zpracovává, včetně aplikací uživatelské procedury.

Bez ohledu na zdroj této adresy může každá aplikace zpracovávající zprávu zvolit použití této adresy pro vrácení odpovědi, stavu nebo zprávy hlášení do původní aplikace.

Způsob, jakým jsou tyto zprávy odezvy směrován, se liší od způsobu, jakým je směrována původní zpráva. Musíte si být vědomi toho, že toky zpráv, které vytvoříte k jiným správcům front, potřebují odpovídající návratové toky.

Konflikty fyzických názvů

Název cílové hodnoty fronty pro odpověď byl vyřešen na název fyzické fronty v původním správci front. Nesmí být znovu rozlišena u odpovídajícího správce front.

Je pravděpodobné, že se mohou vyskytnout problémy s konfliktem názvů, které může být bráněno pouze sítí v rámci sítě ve fyzických a logických názvech front.

Správa překladů názvů front

Při vytváření definice aliasu správce front nebo definice vzdálených front je pro každou zprávu, která tento název obsahuje, provedeno rozpoznávání názvů. Tato situace musí být spravována.

Tento popis je určen pro návrháře aplikací a plánovače kanálů, které se zabývají jednotlivým systémem, který má kanály zpráv pro sousední systémy. Zabere to místní pohled na plánování a řízení kanálů.

Při vytváření definice aliasu správce front nebo definice vzdálených front je pro každou zprávu, která tento název obsahuje, prováděno rozpoznávání názvů bez ohledu na zdroj této zprávy. Chcete-li dohlédnout na tuto situaci, která může zahrnovat velký počet front v síti správce front, zachovávají si následující tabulky:

- Názvy zdrojových front a správců zdrojových front s ohledem na vyřešené názvy front, vyřešených názvů správců front a rozlišených názvů přenosových front s použitím metody rozpoznání
- Názvy zdrojových front s ohledem na:
  - Vyřešené názvy cílových front
  - Vyřešené názvy správce cílových front
  - Přenosové fronty
  - Názvy kanálů zpráv
  - Jména sousedního systému
  - Názvy front pro odpověď

Poznámka: Použití výrazu *source* v tomto kontextu se vztahuje k názvu fronty nebo názvu správce front poskytovaného aplikací nebo programu kanálu při otevírání fronty pro vkládání zpráv.

Příklad každé z těchto tabulek je zobrazen v Tabulka 19 na stránce 188, Tabulka 20 na stránce 189a Tabulka 21 na stránce 189.

Názvy v těchto tabulkách jsou odvozeny z příkladů uvedených v tomto oddíle a tato tabulka není zamýšlena jako praktický příklad rozlišení názvů front v jednom uzlu.

Tabulka 19. Rozlišení názvů front ve správci front QMA

Zdrojová fronta uvedená při otevření fronty	Zdrojový správce front uvedený při otevření fronty	Rozlišený název fronty	Vyřešený název správce front	Vyřešený název přenosové fronty	Typ rozlišení
QA_norm	-	QA_norm	QMB	QMB	Vzdálená fronta
(libovolný)	QMB	-	-	QMB	(není)
QA_norm	-	QA_norm	QMB	TX1	Vzdálená fronta
QB	QMC	QB	QMD	QMB	Alias správce front

Tabulka 20. Rozlišení názvů front ve správci front QMB

Zdrojová fronta uvedená při otevření fronty	Zdrojový správce front uvedený při otevření fronty	Rozlišený název fronty	Vyřešený název správce front	Vyřešený název přenosové fronty	Typ rozlišení
QA_norm	-	QA_norm	QMB	-	(není)
QA_norm	QMB	QA_norm	QMB	-	(není)
QA_norm	PRIORITA QMB_PRIORITY	QA_norm	QMB	-	Alias správce front
(libovolný)	QMC	(libovolný)	QMC	QMC	(není)
(libovolný)	QMD_norm	(libovolný)	QMD_norm	TX1	Alias správce front
(libovolný)	PRIORITA QMD_PRIORITY	(libovolný)	PRIORITA QMD_PRIORITY	QMD_fast	Alias správce front
(libovolný)	QMC_small	(libovolný)	QMC_small	TX_small	Alias správce front
(libovolný)	QMC_large	(libovolný)	QMC_large	TX_externí	Alias správce front
QB_small	QMC	QB_small	QMC	TX_small	Vzdálená fronta
QB_large	QMC	QB_large	QMC	TX_large	Vzdálená fronta
(libovolný)	QME	(libovolný)	QME	TX1	Alias správce front
QA	QMC	QA	QMC	TX1	Vzdálená fronta
QB	QMD	QB	QMD	TX1	Vzdálená fronta

Tabulka 21. Převod názvu fronty odpovědí na název fronty správce front QMA

Návrh aplikací		Definice aliasu pro odpověď	
Lokální správce front	**Název fronty pro zprávy**	**Název aliasu fronty pro odpověď**	**Redefinováno na**
QMA	QRR	OR.	QRR na QMA_class1

Pořadové číslování zpráv kanálu

Kanál používá pořadová čísla, aby zkontroloval, že zprávy jsou doručeny ve stejném pořadí, v jakém byly převzaty z přenosové fronty.

Čísla posloupností kanálů se kontrolují při spuštění kanálu a dojde k neshodě, znamená to, že trvalá data synchronizace byla ztracena na obou stranách kanálu; například konfigurace zotavení z havárie (DR) nebo ukončení dávkového zpracování byla přerušena, když byl kanál v nejistém stavu.

Resetování nebo ignorování neshod pořadových čísel viz **IgnoreSeqNumberMismatch** v části *Sekce kanálů souboru qm.ini*nehrozí riziko ztráty nebo duplikace dávky zpráv, a neobnoví se stav nejistoty kanálu.

Tyto informace lze zobrazit pomocí příkazu DISPLAY CHSTATUS. Pořadové číslo a identifikátor nazývaný LUWID jsou uloženy v trvalém úložišti pro poslední zprávu přenesenou v dávce. Tyto hodnoty se používají během spouštění kanálu, aby se zajistilo, že oba konce vazby souhlasí s tím, že zprávy byly úspěšně přeneseny.

Sekvenční načítání zpráv

Pokud aplikace vkládá posloupnost zpráv do stejné cílové fronty, tyto zprávy mohou být načteny v posloupnosti pomocí aplikace ***jedna*** s posloupností operací MQGET, jsou-li splněny následující podmínky:

- Všechny požadavky na vložení byly provedeny ze stejné aplikace.
- Všechny požadavky na vložení byly buď ze stejné pracovní jednotky, nebo všechny požadavky na vložení byly provedeny mimo jednotku práce.
- Všechny zprávy mají stejnou prioritu.
- Všechny zprávy mají stejnou perzistenci.
- Pro vzdálené fronty je konfigurace taková, že může existovat pouze jedna cesta z aplikace provádějící požadavek na vložení přes správce front, přes interkomunikaci, do cílového správce front a do cílové fronty.
- Zprávy se nevloží do fronty nedoručených zpráv (například, je-li fronta dočasně plná).
- Aplikace, která získává zprávu, neúmyslně mění pořadí načítání, například zadáním konkrétního *MsgId* nebo *CorrelId* nebo použitím priorit zpráv.
- Pouze jedna aplikace provádí operace načtení pro načtení zpráv z cílové fronty. Pokud existuje více než jedna aplikace, tyto aplikace musí být navrženy tak, aby všechny zprávy byly získaovány v každé posloupnosti odeslané odesílající aplikací.

Poznámka: Zprávy z jiných úloh a jednotek práce mohou být provázané s posloupností, a to i tam, kde byla posloupnost vložena v rámci jedné pracovní jednotky.

Pokud tyto podmínky nemohou být splněny a pořadí zpráv na cílové frontě je důležité, pak lze aplikaci naprogramovat, aby používala vlastní pořadové číslo zprávy jako část zprávy, aby se zajistilo pořadí zpráv.

Posloupnost načítání rychlých přechodných zpráv

Přechodné zprávy v rychlém kanálu mohou přepsat trvalé zprávy na stejném kanálu a tak se dostaví mimo pořadí. Přijímající agent MCA okamžitě umístí přechodné zprávy do cílové fronty a zviditelní je. Trvalé zprávy nejsou viditelné až do dalšího bodu synchronizace.

Testování zpětné smyčky

Testování zpětné smyčky je technika na jiných platformách než z/OS , která umožňuje testovat komunikační spojení bez skutečného propojení s jiným počítačem.

Nastavili jste spojení mezi dvěma správci front, jako kdyby byli na samostatných počítačích, ale otestovali jste připojení pomocí cyklu na jiném procesu na stejném počítači. Tato technika znamená, že můžete testovat svůj komunikační kód, aniž byste museli vyžadovat aktivní síť.

Způsob, jakým to uděláte, závisí na tom, které produkty a protokoly používáte.

V systému Windows můžete použít adaptér "loopback".

Další informace naleznete v dokumentaci k produktům, které používáte.

Trasování přenosové cesty a záznam aktivity

Můžete potvrdit trasu, kterou zpráva prochází řadou správců front dvěma způsoby.

Můžete použít aplikaci Trasa zobrazení produktu IBM MQ , která je k dispozici prostřednictvím řídicího příkazu **dspmqrte**, nebo můžete použít záznam aktivity. Obě tato témata jsou popsána v tématu Odkaz na monitorování.

Úvod do distribuované správy front

Distribuovaná správa front (DQM) se používá k definování a řízení komunikace mezi správci front.

Správa distribuovaných front:

- Umožňuje vám definovat a řídit komunikační kanály mezi správci front.
- Poskytuje vám službu kanálu zpráv k přesouvání zpráv z typu *lokální fronty*, známého jako přenosová fronta, do komunikačních linek na lokálním systému a z komunikačních spojení do lokálních front v cílovém správci front.
- Poskytuje nástroje pro monitorování činnosti kanálů a diagnostiku problémů, použití panelů, příkazů a programů.

Definice kanálů přidružují názvy kanálů k přenosových frontách, identifikátorům komunikačního propojení a atributech kanálů. Definice kanálů jsou implementovány různými způsoby na různých platformách. Odesílání a příjem zpráv je řízeno programy známými jako *agenty kanálů zpráv* (MCA), které používají definice kanálů ke spuštění a řízení komunikace.

Kontrolované MCoby jsou řízeny samotným řízením kvality dat. Struktura je závislá na platformě, ale zpravidla obsahuje listenery a monitory spouštěčů, spolu s příkazy a panely operátora.

Kanál zpráv je jednosměrné propojení procesů pro přesouvání zpráv z jednoho správce front do jiného. Takže kanál zpráv má dva koncové body, představované dvojicí jednotek MCA. Každý koncový bod má definici svého konce kanálu zpráv. Jeden konec by například definoval odesilatele, druhý konec příjemce.

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

- ULW “Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 220
- z/OS “Monitorování a řízení kanálů v systému z/OS” na stránce 875
- IBM i “Monitorování a řízení kanálů v systému IBM i” na stránce 244

Příklady plánování kanálů zpráv viz:

- ULW Příklad plánování kanálů zpráv pro produkt UNIX, Linux, and Windows
- IBM i Příklad plánování kanálů zpráv pro produkt IBM i
- z/OS Příklad plánování kanálů zpráv pro produkt z/OS
- z/OS Příklad plánování kanálů zpráv pro produkt z/OS s použitím skupin sdílení front

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

Související pojmy

“Odeslání a příjem zprávy” na stránce 192
Následující obrázek ukazuje model distribuované správy front s podrobnými informacemi o vztazích mezi entitami při přenosu zpráv. Zobrazuje také tok pro řízení.

“Řídicí funkce kanálu” na stránce 199
Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

“Co se stane, když nebude možné zprávu doručit?” na stránce 212
Nelze-li zprávu doručit, může ji agent MCA zpracovat několika způsoby. Může to zkusit znovu, může vrátit odesilateli, nebo to může dát do fronty nedoručených zpráv.

“Inicializační a konfigurační soubory” na stránce 216
Způsob zpracování inicializačních dat kanálu závisí na platformě IBM MQ .

“Převod dat pro zprávy” na stránce 218
Zprávy produktu IBM MQ mohou vyžadovat převod dat při odesílání mezi frontami v různých správcích front.

“Psaní vlastních agentů kanálů zpráv” na stránce 218
IBM MQ vám umožňuje zapsat si vlastní programy MCA (Message Channel Agent) nebo instalovat jeden z nezávislých dodavatelů softwaru.

“Další informace, které je třeba zvážit při správě distribuovaných front” na stránce 219

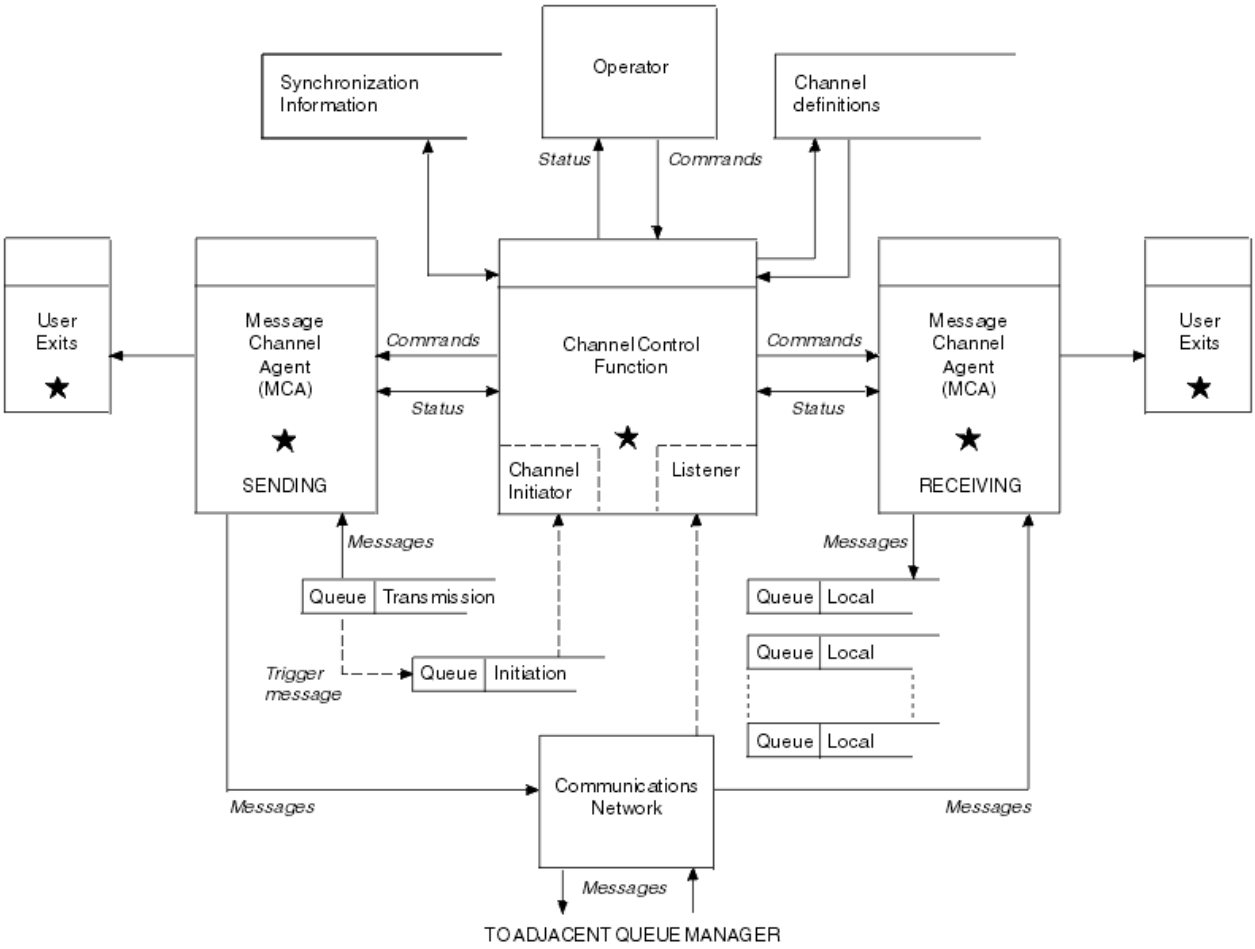
Další témata, která je třeba zvážit při přípravě produktu IBM MQ pro distribuovanou správu front. Toto téma pokrývá frontu nedoručených zpráv, Fronty v použití, Rozšíření systému a programy uživatelských procedur a Spouštění kanálů a listenerů jako ověřené aplikace.

Související odkazy

Příklad konfiguračních informací

Odeslání a příjem zprávy

Následující obrázek ukazuje model distribuované správy front s podrobnými informacemi o vztazích mezi entitami při přenosu zpráv. Zobrazuje také tok pro řízení.



Obrázek 17. Model distribuované správy front

Poznámka:

1. V závislosti na platformě je v závislosti na platformě jedna sběrnice MCA pro kanál. Pro určitého správce front může existovat jedna nebo více řídicích funkcí kanálu.
2. Implementace funkcí MCA a řídicích funkcí kanálu je závislá na platformě. Mohou být programy nebo procesy či podprocesy a mohou se jednat o jednu entitu nebo řadu z nich skládající se z několika nezávislých nebo propojených částí.
3. Všechny komponenty označené hvězdičkou mohou používat rozhraní MQI.

Parametry kanálu

MCA přijímá své parametry jedním z několika způsobů:

- Pokud je příkaz spuštěn příkazem, je v datové oblasti předán název kanálu. Agent MCA poté přečte definici kanálu přímo, aby získal její atributy.

- Pro odesílatele a v některých případech může být agent MCA spuštěn automaticky pomocí spouštěče správce front. Název kanálu je načten z definice procesu spouštěče, je-li to možné, a je předán do agenta MCA. Zbývající zpracování je stejné, jak bylo popsáno dříve. Kanály serveru musí být nastaveny pouze tak, aby se spouštěly, pokud jsou plně kvalifikované, to znamená, že určují hodnotu CONNAME, ke kterému se má připojit.
- Pokud je spuštěno vzdáleně odesilatelem, serverem, klientem nebo připojením klienta, předá se název kanálu v počátečních datech z partnerského agenta kanálu zpráv. Sběrnice MCA čte definici kanálu přímo za účelem získání jeho atributů.

Některé atributy, které nejsou definovány v definici kanálu, jsou také obchodovatelné:

Rozdělit zprávy
Pokud jeden konec nepodporuje rozdělené zprávy, pak se neodesílají rozdělené zprávy.

Schopnost převodu
Pokud jeden konec nemůže provést potřebnou konverzi kódové stránky nebo převod numerického kódování, je-li to nutné, druhý konec jej musí zpracovat. Pokud jej ani koncový bod nepodporuje, kanál nelze spustit.

Podpora seznamu distribuce
Pokud jeden konec nepodporuje distribuční seznamy, partnerský agent MCA nastaví příznak ve své přenosové frontě tak, že bude vědět, že zachytává zprávy určené pro více míst určení.

Stav kanálů a pořadová čísla

Programy agenta kanálu zpráv uchovávají záznamy o aktuálním pořadovém čísle a logické jednotce práce pro každý kanál a o obecném stavu kanálu. Některé platformy vám umožňují zobrazit tyto informace o stavu, které vám pomohou při řízení kanálů.

Jak odeslat zprávu jinému správci front

Tato sekce popisuje nejjednodušší způsob odeslání zprávy mezi správci front, včetně nezbytných předpokladů a požadovaných oprávnění. Další metody lze také použít k odeslání zpráv vzdálenému správci front.

Před odesláním zprávy z jednoho správce front do jiného je třeba provést následující kroky:

1. Zkontrolujte, zda je váš zvolený komunikační protokol k dispozici.
2. Spusťte správce front.
3. Spusťte iniciátory kanálu.
4. Spusťte listenery.

Musíte také mít správnou autorizaci zabezpečení produktu IBM MQ , abyste mohli vytvořit požadované objekty.

Chcete-li odeslat zprávy z jednoho správce front do jiného, postupujte takto:

- Definujte následující objekty ve zdrojovém správci front:
  - Kanál odesílatele
  - Definice vzdálené fronty
  - Inicializační fronta (z/OS povinná na z/OS, jinak volitelné)
  - Přenosová fronta
  - Fronta nedoručených zpráv
- Definujte následující objekty v cílovém správci front:
  - Kanál příjemce
  - Cílová fronta
  - Fronta nedoručených zpráv

K definování těchto objektů můžete použít několik různých metod, v závislosti na vaší platformě IBM MQ :

- Na všech platformách můžete použít příkazy skriptů IBM MQ (MQSC) popsané v Příkazy MQSC programu pro programovatelné příkazy (PCF) popsané v příručce Automatizace administračních úlohnebo v Průzkumníku IBM MQ .
- z/OS V systému z/OSmůžete také použít panely Operace a Ovládací panely popsané v části Administrace produktu IBM MQ for z/OS .
- IBM i V systému IBM imůžete také použít rozhraní panelu.

Další informace o vytváření komponent pro odesílání zpráv do jiného správce front naleznete v následujících dílčích tématech:

Související pojmy

“IBM MQ technologie distribuovaných front” na stránce 172
Dílčí témata v tomto oddílu popisují techniky, které se používají při plánování kanálů. Tato dílčí témata popisují techniky, které vám pomohou naplánovat vzájemné propojení správců front a správu toku zpráv mezi vašimi aplikacemi.

“Úvod do distribuované správy front” na stránce 190
Distribuovaná správa front (DQM) se používá k definování a řízení komunikace mezi správci front.

“Spouštěcí kanály” na stránce 213
Produkt IBM MQ poskytuje službu pro automatické spouštění aplikace, jsou-li splněny určité podmínky ve frontě. Toto zařízení se nazývá spouštění.

“Bezpečnost zpráv” na stránce 211
Kromě typických funkcí zotavení produktu IBM MQzajišťuje distribuovaná správa front, že zprávy jsou řádně doručovány pomocí procedury synchronizačního bodu koordinované mezi dvěma konci kanálu zpráv. Pokud tento postup zjistí chybu, zavře kanál tak, abyste mohli problém vyšetřit a bezpečně uchovávat zprávy v přenosové frontě, dokud nebude kanál restartován.

Související úlohy

“Vytvoření správců front na více platformách” 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 prostředky, které jsou k ní přidruženy, zejména fronty, které vlastní. Poskytuje aplikacím pro volání rozhraní MQI (Message Queuing Interface) volání příkazů a příkazy k vytvoření, úpravě, zobrazení a odstranění objektů IBM MQ .

“Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 220
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 oblastí úložiště pro informace o synchronizaci.

“Monitorování a řízení kanálů v systému IBM i” na stránce 244
Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

“Konfigurace připojení mezi 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 správce front” na stránce 265
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 871
Tato část popisuje přípravy systému IBM MQ for z/OS , které musíte provést, než začnete používat distribuované řazení do front.

Definování kanálů

Chcete-li odeslat zprávy z jednoho správce front do jiného, je třeba definovat dva kanály. Je třeba definovat jeden kanál ve zdrojovém správci front a jeden kanál v cílovém správci front.

Ve zdrojovém správci front

Definujte kanál s typem kanálu SENDER. Je třeba určit následující:

- Název přenosové fronty, která má být použita (atribut XMITQ).
- Název připojení partnerského systému (atribut CONNAME).
- Název komunikačního protokolu, který používáte (atribut TRPTYPE). V systému IBM MQ for z/OSmusí být protokol protokolem TCP nebo LU6.2. Na ostatních platformách tuto volbu nemusíte zadávat. Můžete ji nechat pro výběr hodnoty z vaší výchozí definice kanálu.

Podrobnosti o všech atributech kanálu jsou uvedeny v části Atributy kanálu.

V cílovém správci front

Definujte kanál s typem kanálu RECEIVER a se stejným názvem jako odesílací kanál.

Uveďte jméno komunikačního protokolu, který používáte (atribut TRPTYPE). V systému IBM MQ for z/OSmusí být protokol protokolem TCP nebo LU6.2. Na ostatních platformách tuto volbu nemusíte zadávat. Můžete ji nechat pro výběr hodnoty z vaší výchozí definice kanálu.

Definice přijímacího kanálu mohou být generické. To znamená, že pokud máte několik správců front komunikujících se stejným příjemcem, odesílající kanály mohou pro příjemce zadat stejný název a pro všechny se použije jedna definice příjemce.

Definujete-li kanál, můžete jej otestovat pomocí příkazu PING CHANNEL. Tento příkaz odešle speciální zprávu z odesílacího kanálu do přijímacího kanálu a zkontroluje, zda je vrácena.

Poznámka: Hodnota parametru TRPTYPE je ignorována agentem oznamovacího kanálu zpráv. Např. TRPTYPE of TCP na definici kanálu odesílatele úspěšně začíná s TRPTYPE LU62 v definici kanálu příjemce jako partner.

Definování front

Chcete-li odesílat zprávy z jednoho správce front do jiného, je třeba definovat až šest front. Ve zdrojovém správci front je třeba definovat až čtyři fronty a až dvě fronty v cílovém správci front.

Ve zdrojovém správci front

- Definice vzdálené fronty

  V této definici zadejte následující:

  Název vzdáleného správce front
  Název cílového správce front.

  Název vzdálené fronty
  Název cílové fronty v cílovém správci front.

  Jméno přenosové fronty
  Název přenosové fronty. Tento název přenosové fronty není třeba zadávat. Pokud ji nevytvoříte, použije se přenosová fronta se stejným názvem jako má cílový správce front. Pokud tato hodnota neexistuje, bude použita výchozí přenosová fronta. Doporučuje se, abyste přenosové frontě pojmenoval stejný název jako cílového správce front, aby byla fronta nalezena standardně.

- Definice inicializační fronty

  z/OS To 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 fronty určené v poli názvu vzdálené fronty v definici vzdálené fronty ve zdrojovém správci front.
- Definice fronty nedoručených zpráv

  Definujte frontu nedoručených zpráv, do které lze zapisovat nedoručené zprávy.

Související pojmy

"Vytvoření přenosové fronty" na stránce 196
Než bude možné spustit kanál (jiný než žadatelský kanál), musí být přenosová fronta definována tak, jak je popsáno v této sekci. Přenosová fronta musí být uvedena v definici kanálu.

"Vytvoření přenosové fronty v systému IBM i" na stránce 196
Přenosovou frontu na platformě IBM i můžete vytvořit pomocí panelu Vytvořit frontu MQM.

Vytvoření přenosové fronty

Než bude možné spustit kanál (jiný než žadatelský kanál), musí být přenosová fronta definována tak, jak je popsáno v této sekci. Přenosová fronta musí být uvedena v definici kanálu.

Definujte lokální frontu s atributem USAGE nastaveným na hodnotu XMITQ pro každý odesílající kanál zpráv. Chcete-li ve svých definicích vzdálených front použít určitou přenosovou frontu, vytvořte vzdálenou frontu podle následujícího obrázku.

Chcete-li vytvořit přenosovou frontu, použijte IBM MQ Commands (MQSC), jak je uvedeno v následujících příkladech:

Příklad příkazu pro vytvoření přenosové fronty

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

Příklad příkazu pro vytvoření vzdálené fronty

```
DEFINE QREMOTE(PAYROLL) DESCR('Remote queue for QM2') +
XMITQ(QM2) RNAME(PAYROLL) RQMNAME(QM2)
```

Zvažte pojmenování přenosové fronty ve jménu správce front ve vzdáleném systému, jak je zobrazeno v příkladech.

Vytvoření přenosové fronty v systému IBM i

Přenosovou frontu na platformě IBM i můžete vytvořit pomocí panelu Vytvořit frontu MQM.

Musíte definovat lokální frontu s atributem pole Použití nastaveným na *TMQ, pro každý odesílající kanál zpráv.

Chcete-li použít definice vzdálených front, použijte stejný příkaz k vytvoření fronty typu *RMT a použití *NORMAL.

Chcete-li vytvořit přenosovou frontu, použijte příkaz CRTMQMQ z příkazového řádku a zobrazí se vám první panel vytvoření fronty; viz Obrázek 18 na stránce 197.

```
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 18. Vytvořit frontu (1)

Zadejte název fronty a určete typ fronty, který chcete vytvořit: Lokální, Vzdálený nebo Alias. V případě přenosové fronty zadejte na tomto panelu lokální (*LCL) a stiskněte klávesu Enter.

Zobrazí se druhá stránka panelu Vytvořit frontu MQM, viz Obrázek 19 na stránce 197.

```
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 19. Vytvořit frontu (2)

Změňte kteroukoli z výchozích zobrazených hodnot. Chcete-li přejít na další obrazovku, stiskněte klávesu Page Down, viz Obrázek 20 na stránce 198.

```
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 20. Vytvořit frontu (3)

Zadejte *TMQ, pro přenosovou frontu, v poli Použití tohoto panelu a změňte kteroukoli z předvolených hodnot zobrazených v ostatních polích.

```
Create MQM Queue (CRTMQMQ)

Type choices, press Enter.

Usage . . . . . *TMQ     *SYSDFTQ, *NORMAL, *TMQ
Queue depth high threshold . . .  80      0-100, *SYSDFTQ
Queue depth low threshold . . .  20      0-100, *SYSDFTQ
Queue full events enabled . . .  *YES     *SYSDFTQ, *NO, *YES
Queue high events enabled . . .  *YES     *SYSDFTQ, *NO, *YES
Queue low events enabled . . . .  *YES     *SYSDFTQ, *NO, *YES
Service interval . . . . . 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 21. Vytvořit frontu (4)

Jste-li spokojeni s tím, že pole obsahují správná data, stiskněte klávesu Enter a vytvořte frontu.

Spuštění kanálu

Při vkládání zpráv do vzdálené fronty definované ve zdrojovém správci front jsou tyto zprávy uloženy v přenosové frontě, dokud není kanál spuštěn. Po spuštění kanálu jsou zprávy doručovány do cílové fronty ve vzdáleném správci front.

Spusťte kanál v odesílajícím správci front pomocí příkazu START CHANNEL. Při spuštění odesílajícího kanálu je přijímající kanál automaticky spuštěn (modulem listener) a zprávy se odesílají do cílové fronty. Oba konce kanálu zpráv musí být spuštěny pro zprávy, které mají být přeneseny.

Vzhledem k tomu, že se oba konce kanálu nacházejí v různých správcích front, mohly být definovány s různými atributy. Chcete-li vyřešit všechny rozdíly, je počáteční vyjednávání dat mezi dvěma konci, když

se kanál spouští. Obecně platí, že oba konce kanálu pracují s atributy, které potřebují méně prostředků. To umožňuje větším systémům vyhovět menším prostředkům menších systémů na druhém konci kanálu zpráv.

Odesílající agent MCA rozdělí velké zprávy před jejich odesláním přes kanál. Jsou znovu složeny ve vzdáleném správci front. To není zřejmé uživateli.

Agent MCA může přenášet zprávy pomocí více podprocesů. Tento proces s názvem *pipeling* umožňuje agentovi MCA mnohem efektivněji přenášet zprávy s méně čekacími stavy. Potrubí zlepšuje výkon kanálu.

Řídicí funkce kanálu

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

Příkazy jsou vydávány prostřednictvím panelů, programů nebo z příkazového řádku do řídicí funkce kanálu. Rozhraní panelu také zobrazuje stav kanálu a data definice kanálu. Programovatelné formáty příkazů nebo tyto příkazy IBM MQ (MQSC) a řídicí příkazy, které jsou podrobně popsány v produktu “Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 220, lze použít.

Příkazy spadají do následujících skupin:

- Administrace kanálu
- Řízení kanálů
- Monitorování stavu kanálu

Příkazy administrace kanálů se zabývají definicemi kanálů. Umožňují vám:

- Vytvořit definici kanálu
- Kopírování definice kanálu
- Změnit definici kanálu
- Odstranit definici kanálu

Příkazy pro řízení kanálů spravují činnost kanálů. Umožňují vám:

- Spustit kanál
- Zastavit kanál
- Znovu synchronizovat s partnerem (v některých implementacích)
- Resetovat pořadová čísla zpráv
- Vyřešit neověřnou dávku zpráv
- Ping; odeslání testovací komunikace přes kanál

Monitorování kanálů zobrazuje stav kanálů, například:

- Aktuální nastavení kanálu
- Zda je kanál aktivní nebo neaktivní
- Údaj o tom, zda kanál v synchronizovaném stavu byl ukončen

Související pojmy

Určování problémů pro kanály

Příprava kanálů

Před pokusem o spuštění kanálu zpráv nebo kanálu MQI je třeba připravit kanál. Musíte se ujistit, že všechny atributy lokálních a vzdálených definic kanálů jsou správné a kompatibilní.

Atributy kanálu popisuje definice kanálů a atributy.

Ačkoli jste nastavili explicitní definice kanálů, vyjednávání o kanálu prováděná při spuštění kanálu může přepsat jednu nebo druhou z definovaných hodnot. Toto chování je normální a není zřejmé uživateli a bylo takto uspořádáno tak, aby jinak nekompatibilní definice mohly fungovat společně.

Automatická definice přijímacích kanálů a kanálů připojení k serveru

Pokud v produktu IBM MQ na všech platformách kromě z/OSneexistuje odpovídající definice kanálu, pak pro přijímač nebo kanál připojení serveru, který má povolenu automatickou definici, je definice vytvořena automaticky. Definice je vytvořena pomocí:

1. Vhodná definice kanálu modelu, SYSTEM.AUTO.RECEIVERnebo SYSTEM.AUTO.SVRCONN. Definice modelových kanálů pro automatickou definici jsou stejné jako výchozí nastavení systému, SYSTEM.DEF.RECEIVERa SYSTEM.DEF.SVRCONN, s výjimkou pole popisu, které je "Auto-definováno", následované 49 mezerami. Administrátor systému si může zvolit změnu libovolné části dodaných definic kanálů modelu.
2. Informace z partnerského systému. Hodnoty z partnera se použijí pro název kanálu a hodnotu zalomení pořadového čísla.
3. Ukončovací program kanálu, který můžete použít ke změně hodnot vytvořených funkcí auto-definition. Viz Channel auto-definition exit program.

Popis je potom zkontrolován, aby se určilo, zda byl změněn při ukončení automatické definice, nebo protože definice modelu byla změněna. Pokud je první 44 znaků stále "Automaticky definováno" následovaným počtem 29 mezer, přidá se název správce front. Pokud posledních 20 znaků je stále ve všech mezerových znacích, přidá se místní čas a datum.

Když byla definice vytvořena a uložena, pokračuje se při spuštění kanálu, jako by definice vždy existovala. Velikost dávky, velikost přenosu a velikost zprávy se vyjednává s partnerem.

Definování jiných objektů

Před spuštěním kanálu zpráv musí být oba konce ve svých správcích front definovány (nebo povoleny pro automatickou definici). Přenosová fronta, kterou má sloužit, musí být definována pro správce front na odesílajícím konci. Komunikační spojení musí být definováno a dostupné. Může být nezbytné připravit další objekty produktu IBM MQ , jako jsou definice vzdálených front, definice aliasů správce front a definice alias fronty pro odpověď, k implementaci scénářů popsaných v tématu “Konfigurace distribuovaných front” na stránce 171.

Informace o definování kanálů MQI viz “Definování kanálů MQI” na stránce 28.

Více kanálů zpráv na přenosovou frontu

Je možné definovat více než jeden kanál na přenosovou frontu, ale pouze jeden z těchto kanálů může být aktivní v jednom okamžiku. Zvažte použití této volby pro zajišťování alternativních tras mezi správci front pro vyvážení provozu a akce nápravného připojení k selhání propojení. Přenosová fronta nemůže být použita jiným kanálem, pokud předchozí kanál k jeho použití ukončil v nejistém stavu odeslání dávky zpráv na odesílajícím konci. Další informace viz “Zacházení s nejistými kanály” na stránce 210.

Spuštění kanálu

Kanál může být způsoben k zahájení přenosu zpráv jedním ze čtyř způsobů. Může být:

- Spuštěno operátorem (nikoli přijímačem, přijímačem klastru nebo kanály připojení serveru).
- Spuštěno z přenosové fronty. Tato metoda se vztahuje pouze na odesílací kanály a plně kvalifikované kanály serveru (kanály, které určují pouze CONNAME). Musíte připravit potřebné objekty pro spouštěcí kanály.
- Spouští se z aplikačního programu (nikoli z přijímačů, přijímačů klastru nebo kanálu připojení serveru).
- Spouští se vzdáleně ze sítě odesilatelem, odesilatelem klastru, klientem, serverem nebo kanálem připojení klienta. Přijímací přijímače, přijímače klastru a pravděpodobně i serverový a žadatelský kanál

jsou tímto způsobem spuštěny; takže se jedná o kanály připojení serveru. Samotné kanály již musí být spuštěny (to znamená povoleno).

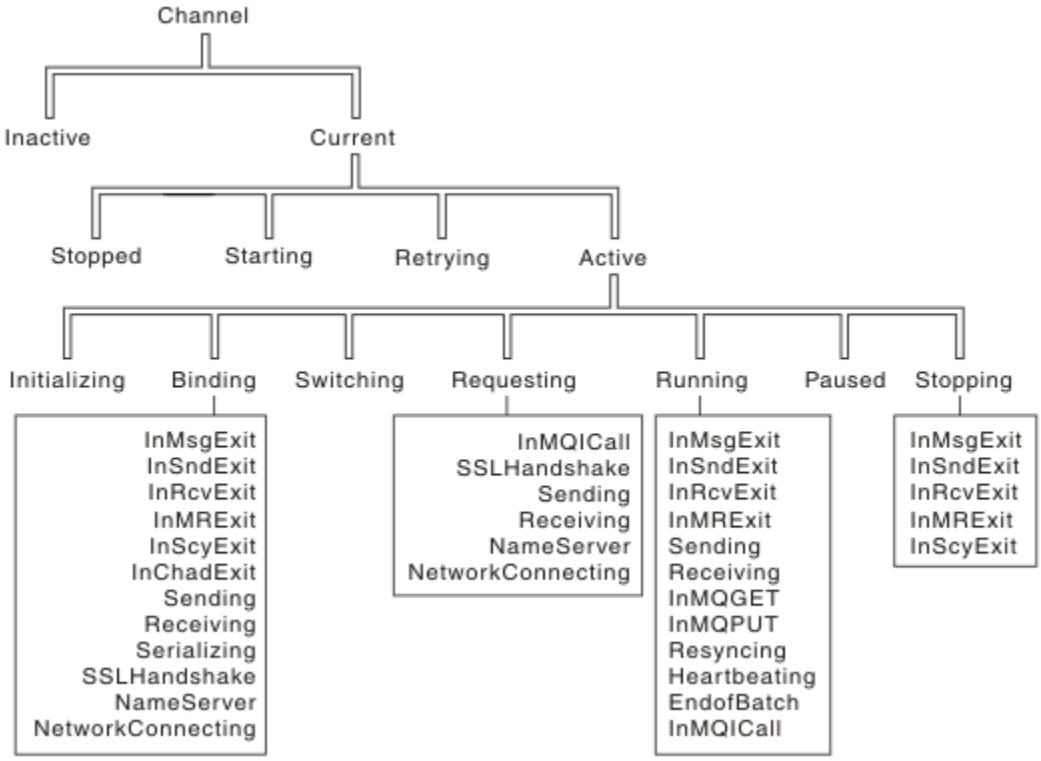
Poznámka: Vzhledem k tomu, že kanál je 'spuštěn', nemusí nutně přenášet zprávy. Místo toho může být 'povoleno' spustit přenos, když se vyskytne jedna ze čtyř událostí popsaných dříve. Povolení a zakázání kanálu je dosaženo pomocí příkazů operátorů START a STOP.

Stavy kanálů

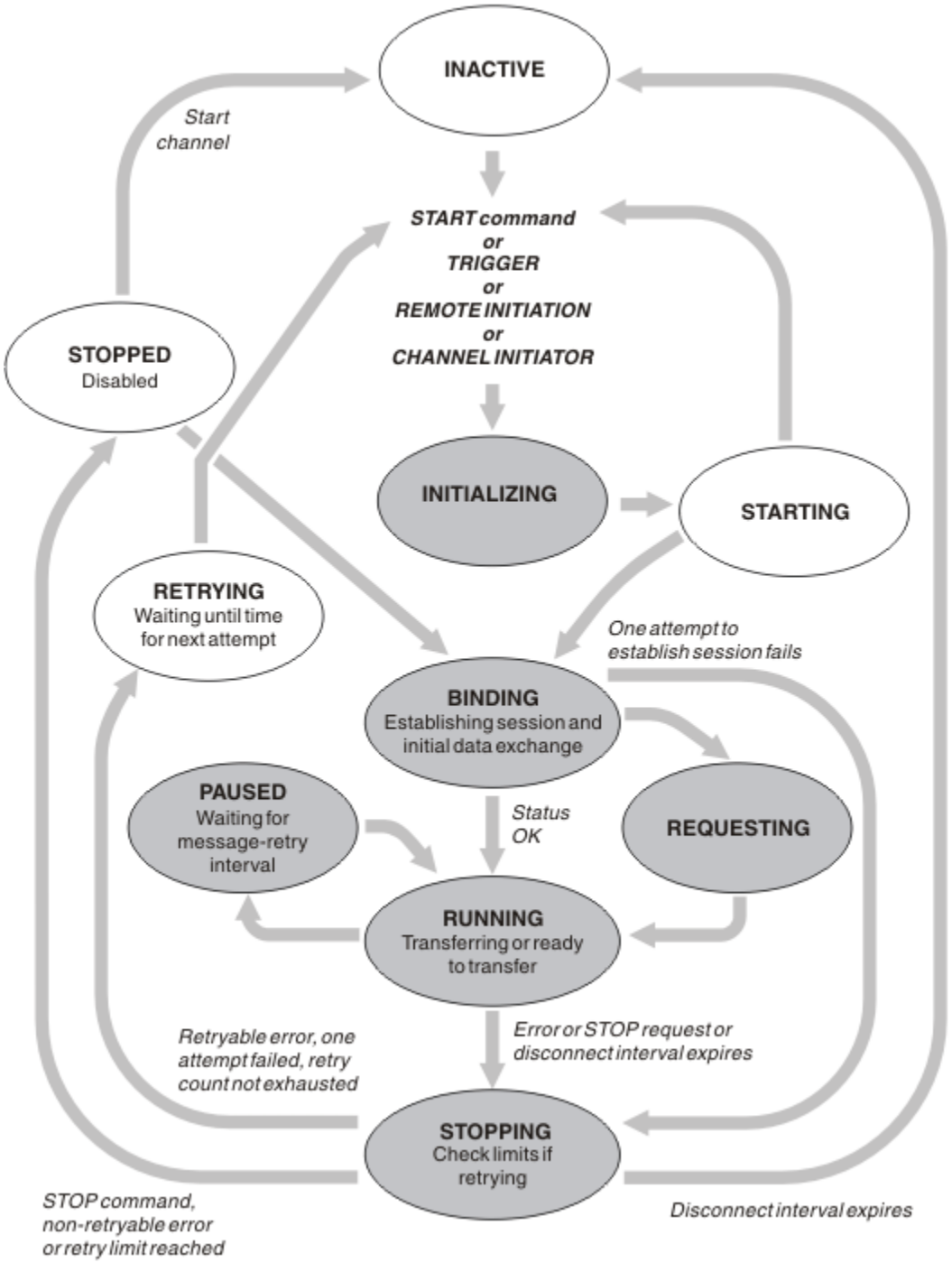
Kanál může být v libovolném okamžiku v některém z mnoha stavů. Některé stavy mají také podstavy. Z daného stavu se kanál může přesunout do jiných stavů.

Obrázek 22 na stránce 201 zobrazuje hierarchii všech možných stavů kanálů a podstavů, které se vztahují ke každému z kanálů kanálu.

Obrázek 23 na stránce 202 zobrazuje odkazy mezi stavy kanálů. Tyto odkazy se vztahují na všechny typy kanálů zpráv a kanálů připojení k serveru.



Obrázek 22. Stavy kanálů a podstavy



Obrázek 23. Toky mezi stavy kanálů

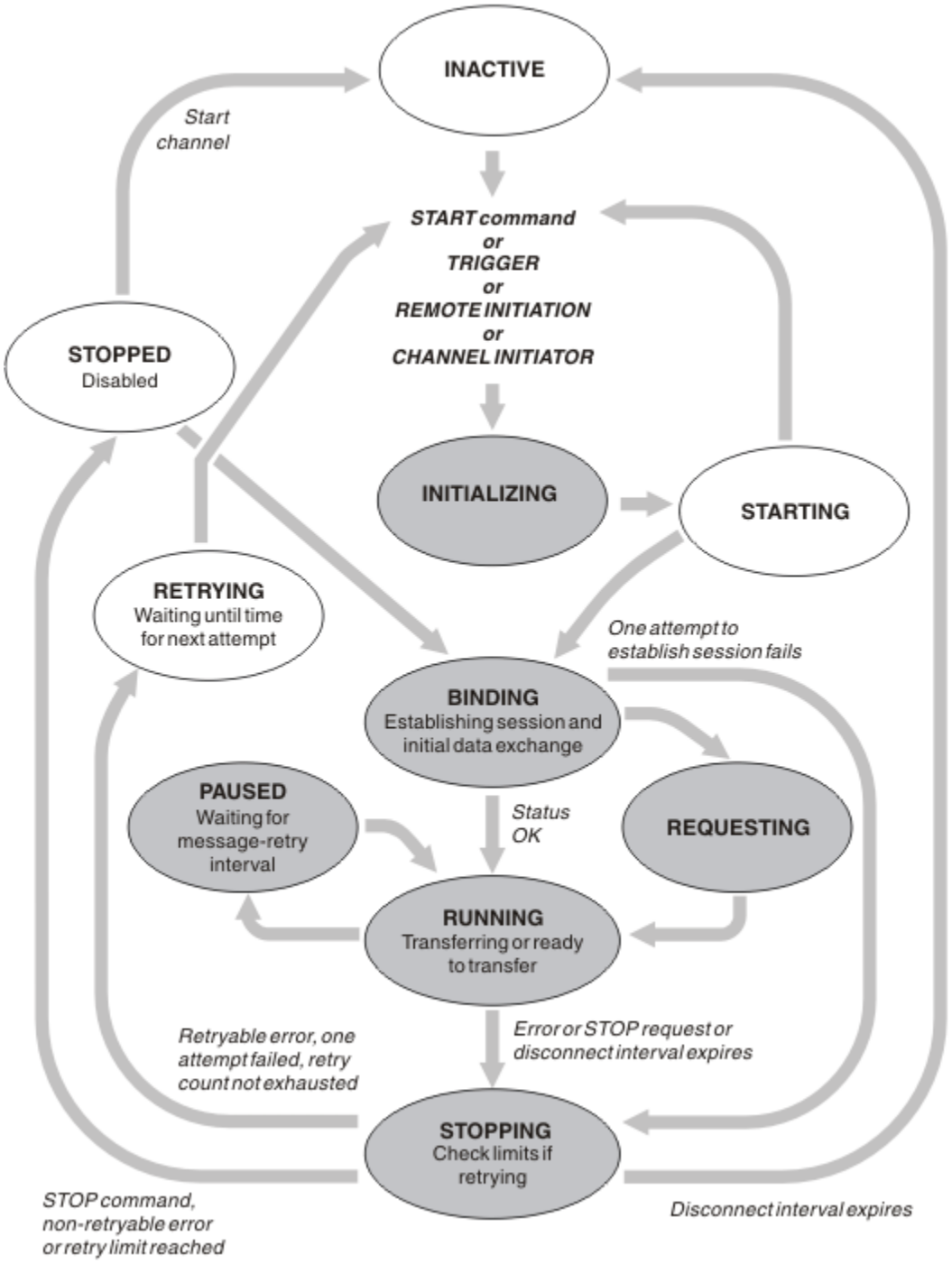
Aktuální a aktivní

Kanál je *aktuální* , je-li ve stavu jiném než neaktivní. Aktuální kanál je *aktivní* , pokud není ve stavu RETRYING, STOPPED nebo STARTING. Je-li kanál aktivní, je spotřebovávat prostředky a je spuštěn proces nebo podproces. Sedm možných stavů aktivního kanálu (INITIALIZING, BINDING, SWITCHING, REQUESTING, RUNNING, PAUSED nebo STOPPING) jsou zvýrazněny v Obrázek 23 na stránce 202.

Aktivní kanál může také zobrazit podstav poskytující více podrobností přesně toho, co kanál dělá. Podstavy pro každý stav jsou zobrazeny v Obrázek 22 na stránce 201.

Aktuální a aktivní
Kanál je "aktuální" , je-li ve stavu jiném než neaktivní. Aktuální kanál je "aktivní" , pokud není ve stavu RETRYING, STOPPED nebo STARTING.

Je-li kanál "aktivní", může také zobrazit podstav poskytující více podrobností přesně toho, co kanál dělá.



Obrázek 24. Toky mezi stavy kanálů

Poznámka:

1. Je-li kanál v jednom ze šesti stavů zvýrazněných v Obrázek 24 na stránce 203 (INITIALIZING, BINDING, REQUESTING, RUNNING, PAUSED nebo STOPPING), spotřebovává se prostředek a je spuštěn proces nebo podproces; kanál je *aktivní*.
2. Je-li kanál ve stavu ZASTAVENO, může být relace aktivní, protože další stav zatím není znám.

Určení maximálního počtu aktuálních kanálů

Můžete uvést maximální počet kanálů, které mohou být aktuální v daném okamžiku. Toto číslo je počet kanálů, které mají položky ve stavové tabulce kanálu, včetně kanálů, které se opakují, a kanálů, které jsou zastaveny. Uveďte tuto hodnotu pro vaši platformu:

- z/OS Použijte příkaz `ALTER QMGR MAXCHL` .
- IBM i Upravte inicializační soubor správce front.
- Linux UNIX Upravte konfigurační soubor správce front.
- Použijte IBM MQ Explorer.

Další informace o hodnotách nastavených pomocí inicializačního programu nebo konfiguračního souboru naleznete v tématu Stanzy konfiguračního souboru pro distribuované řazení do fronty. Další informace o určení maximálního počtu kanálů naleznete v následujících tématech:

- ULW Administrace produktu IBM MQ.
- IBM i Administrace produktu IBM MQ for IBM i.
- z/OS Administrace produktu IBM MQ for z/OS.

Poznámka:

1. Kanály připojení serveru jsou zahrnuty v tomto počtu.
2. Kanál musí být aktuální, dříve než může být aktivní. Pokud je kanál spuštěn, ale nemůže se stát aktuální, spuštění se nezdaří.

Určení maximálního počtu aktivních kanálů

Můžete také uvést maximální počet aktivních kanálů, abyste zabránili přetížení systému mnoha spouštěnými kanály. Použijete-li tuto metodu, nastavte atribut intervalu odpojení na nízkou hodnotu, aby bylo možné spustit čekání kanálů, jakmile budou ukončeny další kanály.

Pokaždé, když se kanál, který se opakovaně pokouší navázat spojení s partnerem, stane aktivním kanálem, musí se stát aktivním kanálem. Pokud dojde k selhání pokusu, zůstane aktuální kanál, který není aktivní, dokud se nepokusí o další pokus. Počet opakovaných pokusů kanálu a četnost, která je určena počtem opakování a atributy kanálu intervalu opakování opakování. Pro oba tyto atributy existují krátké a dlouhé hodnoty. Další informace naleznete v tématu Atributy kanálu .

Když se kanál musí stát aktivním kanálem (protože byl vydán příkaz START nebo proto, že byl spuštěn nebo protože nastal čas pro další pokus o zopakování), ale nelze tak učinit, protože počet aktivních kanálů je již na maximální hodnotě, kanál čeká, dokud nebude jeden z aktivních slotů uvolněn jinou instancí kanálu, která přestane být aktivní. Pokud se však kanál spouští, protože je spouštěn vzdáleně, a v té době nejsou k dispozici žádné aktivní sloty, je vzdálené zahájení zamítnuto.

Kdykoli se kanál, který je jiný než žadatelský kanál, pokouší stát se aktivním, přejde do stavu STARTING. Tento stav se vyskytuje i v případě, že je aktivní slot okamžitě dostupný, i když je ve stavu STARTING pouze krátkou dobu. Pokud však musí kanál čekat na aktivní slot, je ve stavu STARTING, zatímco čeká.

Kanály žadatele nepůjdou do stavu STARTING. Pokud nelze spustit žadatelský kanál, protože počet aktivních kanálů je již na limitu, kanál se ukončí nestandardně.

Kdykoli kanál, který není žadatelovým kanálem, nedokáže získat aktivní slot, a tak čeká na první zprávu, zapíše se zpráva do protokolu z/OS nebo konzole z/OS , a vygeneruje se událost. Je-li slot později uvolněn a kanál je schopen získat, vygeneruje se další zpráva a událost. Ani jedna z těchto událostí a zpráv se negeneruje, je-li kanál schopen přímo získat slot.

Je-li příkaz STOP CHANNEL zadán v době, kdy kanál čeká na aktivaci, kanál přejde do stavu STOPPED. Vyzvedne se událost Kanál-Stopped.

Kanály připojení k serveru jsou zahrnuty v maximálním počtu aktivních kanálů.

Další informace o určení maximálního počtu aktivních kanálů naleznete v následujících tématech:

- ULW Administrace produktu IBM MQ.
- IBM i Administrace produktu IBM MQ for IBM i.
- z/OS Administrace produktu IBM MQ for z/OS.

Chyby kanálu
Chyby na kanálech způsobí, že kanál zastaví další přenosy. Je-li kanálem odesilatel nebo server, přejde do stavu RETRY, protože je možné, že se problém může vymazat sám. Pokud nelze přejít do stavu RETRY, kanál přejde do stavu ZASTAVENO.

V případě posílání kanálů je přidružená přenosová fronta nastavena na GET (DISABLED) a spuštění je vypnuto. (Příkaz STOP s hodnotou STATUS (STOPPED) převezme stranu, která ji vydala do stavu ZASTAVENO; pouze expirace intervalu odpojení nebo příkazu STOP s hodnotou STATUS (INACTIVE) jej ukončí normálně a stane se neaktivním.) Kanály, které jsou ve stavu ZASTAVENO, potřebují zásah operátora, než se mohou znovu spustit (viz “Restartování zastavených kanálů” na stránce 210).

Poznámka: Pro systémy IBM i IBM i, UNIX, Linux, and Windows musí být spuštěn inicializátor kanálu, aby se pokus o pokus o pokus pokusil. Není-li inicializátor kanálu k dispozici, bude kanál neaktivní a musí být restartován ručně. Pokud používáte skript ke spuštění kanálu, ujistěte se, že inicializátor kanálu je spuštěn před tím, než se pokusíte spustit skript.

Počet dlouhých opakování (LONGRTY) popisuje, jak probíhá opakování prací. Je-li chyba vymazána, kanál se restartuje automaticky a přenosová fronta je znovu povolena. Je-li dosažen limit opakování bez vymazání chyby, kanál přejde do stavu ZASTAVENO. Zastavený kanál musí být ručně restartován operátorem. Je-li chyba stále přítomna, neopakuje pokus znovu. Když se úspěšně spustí, přenosová fronta je znovu povolena.

z/OS Pokud se inicializátor kanálu zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu inicializátoru kanálu. Stav kanálu pro typ kanálu SVRCONN se však resetuje, pokud se zastaví inicializátor kanálu v době, kdy je kanál ve stavu ZASTAVENO.

Multi Pokud se správce front zastaví v případě, že se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu správce front. Od verze IBM MQ 8.0 se tato vztahuje také na kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

Pokud kanál nemůže vložit zprávu do cílové fronty, protože je tato fronta plná nebo byla zablokována, může kanál zopakovat operaci (uvedený v atributu počtu opakování zprávy) v časovém intervalu (uvedený v atributu intervalu opakování zprávy). Případně můžete napsat vlastní proceduru opakování zpráv, která určuje, které okolnosti způsobí opakovaný pokus, a počet provedených pokusů. Kanál přejde do stavu PAUSED při čekání na dokončení intervalu opakování zprávy.

Chcete-li získat informace o atributech kanálu a o Kanály-uživatelské programy pro kanály systému zpráv informace o ukončení opakování zprávy, prohlédněte si příručku Atributy kanálu a informace o nich.

Limity kanálu připojení serveru

Můžete nastavit limity kanálu pro připojení k serveru, které zabrání klientským aplikacím v vyčerpání prostředků kanálu správce front pomocí parametru **MAXINST** a zabránit tak, aby jedna klientská aplikace byla vyčerpáním kapacity kanálu připojení serveru s parametrem **MAXINSTC** .

Nastavili jste **MAXINST** a **MAXINSTC** příkazem **DEFINE CHANNEL** .

Maximální celkový počet kanálů může být v každém okamžiku ve správci front aktivní. Celkový počet instancí kanálu připojení serveru je zahrnut v maximálním počtu aktivních kanálů.

Nezadáte-li maximální počet současně existujících instancí kanálu připojení serveru, který lze spustit, je možné použít jedinou klientskou aplikaci, která se připojuje k jednomu kanálu připojení serveru, aby vyčerpat maximální počet aktivních kanálů, které jsou k dispozici. Když je dosaženo maximálního počtu

aktivních kanálů, zabrání spuštění jakýchkoli jiných kanálů ve správci front. Chcete-li se této situaci vyhnout, musíte omezit počet souběžných instancí jednotlivého kanálu připojení serveru, který může být spuštěn bez ohledu na to, který klient je spustil.

Je-li hodnota limitu omezena na pod aktuálně spuštěným počtem instancí kanálu pro připojení k serveru, dokonce i na nulu, spuštěné kanály nebudou ovlivněny. Nové instance nelze spustit, dokud nebudou úspěšně spuštěny dostatečné existující instance, takže počet momentálně spuštěných instancí je menší než hodnota limitu.

Mnoho různých kanálů připojení klienta se také může připojit k jednotlivým kanálům připojení serveru. Limit počtu současných instancí jednotlivého kanálu připojení serveru, který může být spuštěn bez ohledu na to, který klient je spustil, zabrání klientovi v vyčerpání maximální kapacity aktivního kanálu správce front. Pokud také neomezíte počet simultánních instancí jednotlivých kanálů připojení k serveru, které lze spustit z jednoho klienta, pak je možné, aby jedna, vadná klientská aplikace otevřela tolik připojení, že vyčerpá kapacitu kanálu alokovanou pro jednotlivé kanály připojení serveru, a zabrání tak dalším klientům, kteří potřebují připojení k tomuto kanálu, aby mohli používat kanál. Chcete-li se této situaci vyhnout, je třeba omezit počet současně existujících instancí jednotlivých kanálů připojení serveru, které lze spustit z jednotlivých klientů.

Je-li hodnota individuálního limitu klienta redukována pod počet instancí kanálu připojení serveru, které momentálně běží od jednotlivých klientů, dokonce i na nulu, spuštěné kanály nejsou ovlivněny. Nové instance kanálu připojení serveru však nelze spustit z jednoho klienta, který překračuje nový limit, dokud nebudou spuštěné dostatečné existující instance z tohoto klienta, takže počet momentálně spuštěných instancí je menší než hodnota tohoto parametru.

Související odkazy

Atributy kanálu 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

Pokud v systému IBM MQ for z/OSpoužíváte protokol TCP/IP jako přenosový protokol, můžete také zadat hodnotu pro atribut kanálu intervalu **Keepalive** (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).

Pokud v systému IBM MQ for IBM i, UNIX, 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 příjmu* , se určuje podle hodnoty HBINT (interval prezenčního signálu).

V systémech IBM MQ for IBM i, UNIX, Linux, and Windows je hodnota *vypršení časového limitu příjmu* nastavena takto:

1. U počátečního počtu toků je před zahájením vyjednávání hodnota *časového limitu pro příjem* dvojnásobkem hodnoty HBINT z definice kanálu.
2. Jakmile kanály vyjednají hodnotu HBINT, je-li hodnota HBINT nastavena na méně než 60 sekund, hodnota *vypršení časového limitu příjmu* se nastaví na dvojnásobek této hodnoty. Pokud je hodnota HBINT nastavena na 60 sekund nebo více, hodnota *vypršení časového limitu příjmu* je nastavena na 60 sekund větší než hodnota HBINT.

V produktu IBM MQ for z/OSje hodnota *vypršení časového limitu pro příjem* nastavena takto:

1. U počátečního počtu toků je před zahájením vyjednávání hodnota *časového limitu pro příjem* dvojnásobkem hodnoty HBINT z definice kanálu.
2. Je-li nastavena hodnota RCVTIME, je časový limit nastaven na jednu z následujících možností:
   - vyjednané HBINT vynásobené konstantou
   - vyjednaný HBINT plus konstantní počet sekund
   - konstantní počet sekund

   v závislosti na parametru RCVTTYPE a s výhradou případného omezení stanoveného RCVTMIN. RCVTMIN se nepoužije, když je nakonfigurován 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 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 parametru SHARECNV není nula, klient používá plně duplexní připojení, což znamená, že klient může (a dělá) prezenční signál během všech volání MQI.
5. V kanálech klienta IBM WebSphere MQ 7 mohou prezenční signály proudit jak ze serveru, tak ze strany klienta. Časový limit na obou koncích je založen na 2*HBINT pro HBINTy kratší než 60 sekund a HBINT+60 pro HBINTy delší než 60 sekund.
6. 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 pro odeslání nebo příjem, čeká přijímající strana pouze 2 sekundy před zrušením kanálu. Pokud agent MCA provádí úlohu, jako je například šifrování zprávy, může být tato hodnota příliš krátká.

Navrhovaná nastavení

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 naleznete v části ALTER QMGR a IBM MQ dostupnost sítě .

Pokud by se adresa IP odesilatele mohla přeložit na více než jednu adresu, možná budete muset nastavit volbu ADOPTCHK na QMNAME spíše než ALL.

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 Channels souboru qm.ini” na stránce 108 .

Pokud se adresa IP odesilatele může přeložit na více než jednu adresu, možná budete muset nastavit **AdoptNewMCACheck** na `QMNAME` namísto `ALL`.

Převzetí agenta MCA

Funkce Převzetí agenta MCA umožňuje produktu IBM MQ zrušit přijímací kanál a spustit nový na jeho místě.

Pokud kanál ztratí kontakt, kanál příjemce může být ponechán ve stavu 'příjem komunikace'. Když je komunikace znovu zavedena, kanál odesílatele se pokusí znovu navázat spojení. Pokud vzdálený správce front zjistí, že je kanál příjemce již spuštěn, nebude moci spustit jinou verzi téhož kanálu příjemce. Tento problém vyžaduje zásah uživatele k nápravě problému nebo použití systému keepalive.

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

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 tak, aby byly přerušitelné spojení mezi správci front se spořádaným ukončením řízeným pouze atributem kanálu přerušení připojení. Tento mechanizmus funguje dobře, pokud operátor nemusí před vypršením časového intervalu odpojení ukončit kanál. K této potřebě může dojít v následujících situacích:

- Uvedení do klidu
- Ochrana prostředků
- Jednostranná akce na jednom konci kanálu

V takovém případě můžete kanál zastavit. Můžete to provést pomocí:

- v příkazu STOP CHANNEL MQSC

- příkaz Stop Channel PCF
- Průzkumník IBM MQ
- z/OS IBM i jiné mechanismy specifické pro jednotlivé platformy:

  z/OS **Pro z/OS:**
  Panel Zastavení kanálu

  IBM i **Pro IBM i:**
  CL příkaz ENDMQMCHL nebo parametr END na panelu WRKMQMCHL

Pro zastavení kanálů pomocí těchto příkazů jsou k dispozici tři možnosti:

QUIESCE
Volba QUIESCE se pokouší ukončit aktuální dávku zpráv před zastavením kanálu.

Vynutit
Volba FORCE se pokouší okamžitě zastavit kanál a může vyžadovat opětovnou synchronizaci kanálu při restartu, protože kanál může být ponechán na pochybách.

z/OS V systému IBM MQ for z/OSFORCE přeruší probíhající opětovné přidělení zpráv, což může zanechat BIND_NOT_FIXED zpráv částečně přealokovaná nebo mimo pořadí.

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

z/OS V systému IBM MQ for z/OSTERMINATE přeruší probíhající opětovné přidělení zpráv, což může zanechat BIND_NOT_FIXED zprávy částečně přealokovaná nebo mimo pořadí.

Všechny tyto volby opustí kanál ve stavu STOPPED, které vyžadují zásah operátora k jeho restartování.

Zastavení kanálu na odesílajícím konci je efektivní, ale vyžaduje zásah operátora k restartování. Na přijímajícím konci kanálu jsou věci mnohem obtížnější, protože agent MCA čeká na data z odesílající strany a neexistuje žádný způsob, jak zahájit *spořádaný* ukončení kanálu z přijímající strany; příkaz pro zastavení bude nevyřízený až do doby, než se agent MCA vrátí z dat.

V důsledku toho existují tři doporučené způsoby použití kanálů v závislosti na požadovaných provozních charakteristikách:

- Chcete-li, aby vaše kanály byly přerušitelné, uvědomte si, že může dojít k řádnému ukončení pouze z odesílajícího konce. Když jsou kanály přerušeny, je to zastaveno, je nutný zásah operátora (příkaz START CHANNEL), aby je bylo možné restartovat.
- Chcete-li, aby byly kanály aktivní pouze v případě, že pro ně existují zprávy, které mají být přeneseny, nastavte interval odpojení na poměrně nízkou hodnotu. Výchozí nastavení je vysoké, a proto se nedoporučuje pro kanály, kde je tato úroveň řízení požadována. Vzhledem k tomu, že je obtížné přerušení přijímacího kanálu přerušovat, je nejhospodárnější volbou kanál automaticky odpojit a znovu se připojit, jak se pracovní zátěž vyžaduje. U většiny kanálů může být vhodné nastavení intervalu odpojení heuristicky vytvořeno.
- Pomocí atributu intervalu prezenčního signálu můžete způsobit, že odesílající agent MCA odešle tok synchronizačních signálů do přijímajícího agenta MCA během období, ve kterém nemá žádné zprávy k odeslání. Tato akce uvolní přijímajícího agenta MCA ze svého stavu čekání a dává mu možnost uvést kanál do klidového stavu bez čekání na vypršení časového limitu odpojení. Nastavte interval prezenčního signálu o nižší hodnotu, než je hodnota intervalu odpojení.

  Poznámka:

  1. Doporučuje se nastavit interval odpojení na nízkou hodnotu, nebo použít prezenční signály pro kanály serveru. Tato nízká hodnota znamená povolení pro případ, kdy se kanál žadatele ukončí abnormálně (například proto, že kanál byl zrušen), když nejsou k dispozici žádné zprávy pro kanál serveru k odeslání. Je-li interval odpojení nastaven na vysoké a prezenční signály se nepoužívají, server nedetekuje, že žadatel skončil (což bude provádět pouze při příštím pokusu o odeslání zprávy žadateli). Je-li server stále spuštěn, má otevřenou přenosovou frontu pro výhradní vstup, aby bylo možné získat další zprávy, které dorazí do fronty. Je-li učiněn pokus o restartování kanálu od

žadatele, požadavek na spuštění obdrží chybu, protože server má stále otevřenou přenosovou frontu pro výhradní vstup. Je třeba zastavit kanál serveru a poté znovu spustit kanál z klienta.

Restartování zastavených kanálů

Když kanál přejde do stavu STOPPED, je nutné kanál restartovat ručně.

Informace o této úloze

V případě odesílatelů nebo kanálů serveru, kdy kanál vstoupil do stavu STOPPED, byla přidružená přenosová fronta nastavena na GET (DISABLED) a spuštění bylo vypnuto. Když je přijat požadavek na spuštění, tyto atributy se resetují automaticky.

z/OS Pokud se inicializátor kanálu zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu inicializátoru kanálu. Stav kanálu pro typ kanálu SVRCONN se však resetuje, pokud se zastaví inicializátor kanálu v době, kdy je kanál ve stavu ZASTAVENO.

Multi Pokud se správce front zastaví v případě, že se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu správce front. Od verze IBM MQ 8.0 se tato vztahuje také na kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

Procedura

- Restartujte kanál jedním z následujících způsobů:
  - Pomocí příkazu START CHANNEL MQSC.
  - Pomocí příkazu Start Channel PCF command.
  - Pomocí agentaIBM MQ Explorer
  - z/OS V systému z/OSpomocí příkazu Spustit panel kanálu.
  - IBM i V systému IBM ipoužijte buď příkaz STRMQMCHL CL nebo volbu START na panelu WRKMQMCHL.

Zacházení s nejistými kanály

Pochybný kanál je kanál, který má pochybnosti se vzdáleným kanálem o tom, které zprávy byly odeslány a přijaty.

Všimněte si, že rozdíl mezi tímto a správcem front je nejistý o tom, které zprávy by měly být potvrzeny do fronty.

Pomocí parametru kanálu Dávkový prezenční signál (BATCHHB) můžete snížit příležitost pro kanál, který má být umístěn v nejistém stavu. Je-li zadána hodnota tohoto parametru, kanál odesílatele před provedením dalších akcí kontroluje, zda je vzdálený kanál ještě aktivní. Pokud není přijata žádná odezva, kanál příjemce se považuje za již neaktivní. Zprávy lze odvolat, znovu směrovat a odesílací kanál nepochybuje. To snižuje dobu, kdy může být kanál umístěn v nejistém stavu mezi odesílacím kanálem, který ověřuje, zda je kanál příjemce stále aktivní, a ověřením, zda kanál příjemce obdržel odeslané zprávy. Další informace o parametru prezenčního signálu dávky naleznete v tématu Atributy kanálu .

Problémy s nejistým kanálem se obvykle řeší automaticky. I když je komunikace ztracena a kanál je umístěn v nejistém stavu s dávkou zprávy u odesílatele s neznámým stavem příjemky, je situace vyřešena při opětovném navázání komunikace. Záznamy pořadových čísel a LUWID jsou uchovány pro tento účel. Kanál bude nejistý, dokud nebudou vyměněny informace o LUWID a pouze jedna dávka zpráv může mít pochybnosti o kanálu.

Je-li to nezbytné, můžete kanál znovu synchronizovat ručně. Termín *ruční* zahrnuje použití operátorů nebo programů, které obsahují příkazy správy systému IBM MQ . Proces ruční synchronizace funguje následujícím způsobem. Tento popis používá příkazy MQSC, ale můžete také použít ekvivalenty PCF.

1. Použijte příkaz DISPLAY CHSTATUS k vyhledání poslední potvrzené logické pracovní jednotky ID (LUWID) pro ***každou*** stranu kanálu. Toto proveďte pomocí následujících příkazů:
   - Pro nejistou stranu kanálu:

     ```
     DISPLAY CHSTATUS( name ) SAVED CURLUWID
     ```

     Pro další identifikaci kanálu můžete použít parametry CONNAME a XMITQ.
   - Pro přijímající stranu kanálu:

     ```
     DISPLAY CHSTATUS( name ) SAVED LSTLUWID
     ```

     Parametr CONNAME můžete použít k dalšímu označení kanálu.

   Příkazy jsou odlišné, protože pouze odesílající strana kanálu může být nejistá. Přijímající strana není nikdy na pochybách.

   V systému IBM MQ for IBM ilze příkaz DISPLAY CHSTATUS spustit ze souboru pomocí příkazu STRMQMQMMQSC nebo pomocí příkazu Práce se stavem kanálu MQM na příkazu WRKMQMCHST.
2. Jsou-li dvě jednotky LUWID stejné, přijímající strana spáchala jednotku práce, kterou odesílatel považuje za nejistou. Odesílající strana nyní může odstranit nejisté zprávy z přenosové fronty a znovu ji povolit. To se provádí s následujícím příkazem kanálu RESOLVE:

   ```
   RESOLVE CHANNEL( name ) ACTION(COMMIT)
   ```
3. Pokud se obě LUWID liší, přijímající strana nepotvrdila jednotku práce, kterou odesílatel považuje za nejistou. Odesílající strana musí uchovávat nejisté zprávy v přenosové frontě a znovu je odeslat. To se provádí s následujícím příkazem kanálu RESOLVE:

   ```
   RESOLVE CHANNEL( name ) ACTION(BACKOUT)
   ```

   IBM i V systému IBM MQ for IBM imůžete použít příkaz Vyřešit kanál MQM, RSVMQMCHL.

Jakmile je tento proces dokončen, kanál již není na pochybách. V případě potřeby může být přenosová fronta v případě potřeby použita jiným kanálem.

Bezpečnost zpráv

Kromě typických funkcí zotavení produktu IBM MQzajišťuje distribuovaná správa front, že zprávy jsou řádně doručovány pomocí procedury synchronizačního bodu koordinované mezi dvěma konci kanálu zpráv. Pokud tento postup zjistí chybu, zavře kanál tak, abyste mohli problém vyšetřit a bezpečně uchovávat zprávy v přenosové frontě, dokud nebude kanál restartován.

Procedura synchronizačního bodu má výhodu, že se pokusí o zotavení situace *v nejistém stavu* při spuštění kanálu. (*Nejisté* je stav jednotky zotavení, pro kterou byl požadován synchronizační bod, ale výsledek požadavku není dosud znám.) Také přidružené k tomuto zařízení jsou tyto dvě funkce:

1. Vyřešit s potvrzením nebo vyřazováním
2. Vynulovat pořadové číslo

Použití těchto funkcí probíhá pouze ve výjimečných případech, protože kanál se automaticky obnovuje ve většině případů.

Rychlé, přechodné zprávy

Atribut kanálu přechodných zpráv (NPMSPEED) lze použít k určení, že jakékoli přechodné zprávy na kanálu mají být dodány rychleji. Další informace o tomto atributu najdete v tématu Nedodtrvalá rychlost zpráv (NPMSPEED).

Pokud se kanál ukončí během rychlého, netrvalé zprávy jsou v režimu přenosu, zprávy mohou být ztraceny a je na aplikaci, aby bylo možné provést jejich obnovu, je-li to nutné.

Pokud přijímající kanál nemůže vložit zprávu do své cílové fronty, pak je umístěn do fronty nedoručených zpráv, pokud byla definována. Pokud ne, zpráva se vyřadí.

Poznámka: Pokud druhý konec kanálu tuto volbu nepodporuje, kanál se spustí s normální rychlostí.

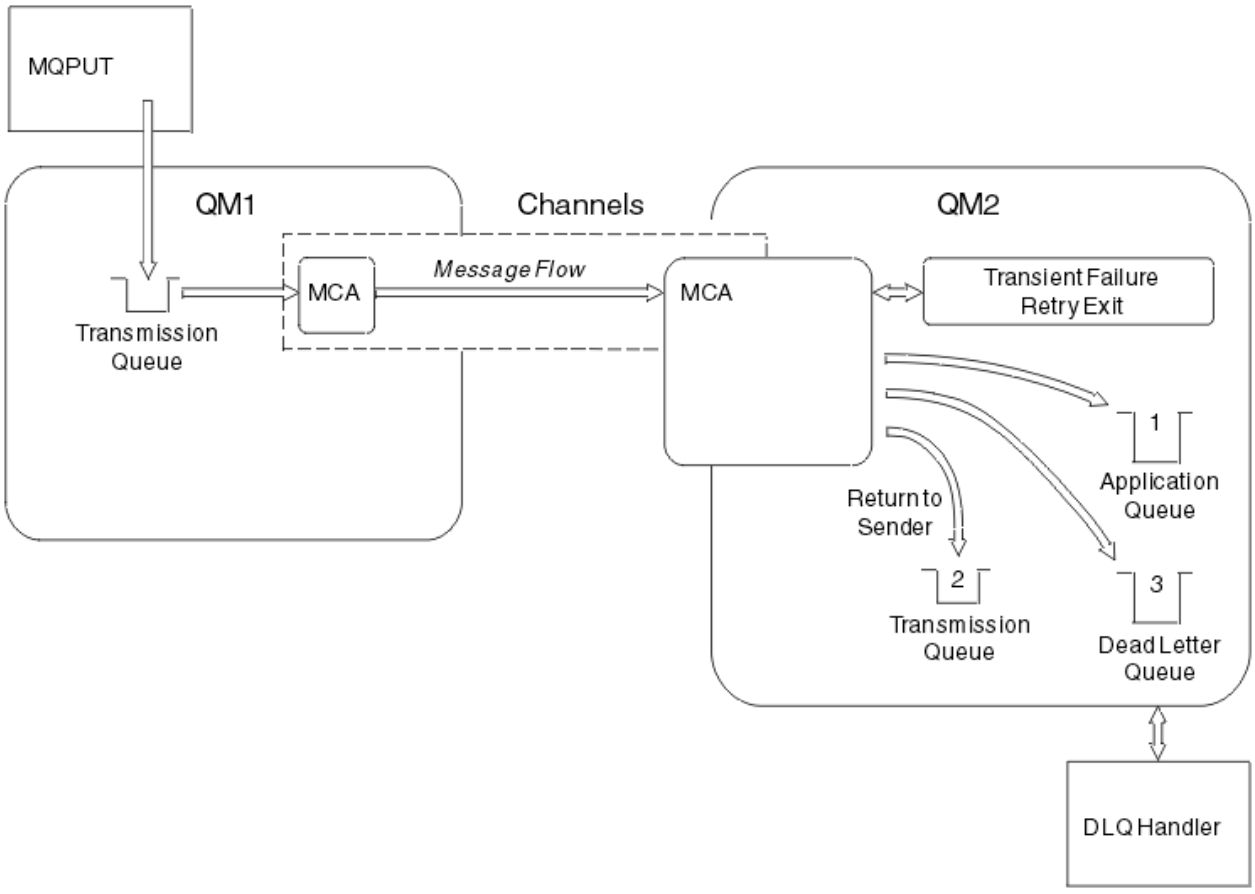
Nedoručené zprávy

Další informace o tom, co se stane, když nelze doručit zprávu, najdete v tématu "Co se stane, když nebude možné zprávu doručit?" na stránce 212.

Co se stane, když nebude možné zprávu doručit?

Nelze-li zprávu doručit, může ji agent MCA zpracovat několika způsoby. Může to zkusit znovu, může vrátit odesilateli, nebo to může dát do fronty nedoručených zpráv.

Obrázek 25 na stránce 212 uvádí zpracování, které se vyskytne, když agent MCA nemůže vložit zprávu do cílové fronty. (Zobrazené volby se nepoužijí na všechny platformy.)



Obrázek 25. Co se stane, když nelze doručit zprávu

Jak je zobrazeno na obrázku, agent MCA může provádět několik věcí se zprávou, kterou nemůže doručit. Tato akce je určena volbami zadanými při definování kanálu a voleb sestavy MQPUT pro danou zprávu.

1. opakování zprávy

   Pokud nemůže agent MCA zařadit do cílové fronty zprávu z příčiny, která by mohla být přechodná (například proto, že je fronta plná), může agent MCA počkat a později zkusit operaci zopakovat. Můžete určit, zda agent MCA čeká, na jak dlouho a kolikrát se to pokusí.

- Při definování kanálu můžete zadat čas opakování zprávy a interval pro chyby MQPUT. Pokud zprávu nelze vložit do cílové fronty, protože je fronta plná nebo je pro vkládání zablokována, program MCA se pokusí o počet zadaných časů v zadaném časovém intervalu.
- Můžete napsat vlastní uživatelskou proceduru pro opakování zpráv. Uživatelská procedura vám umožňuje určit, za jakých podmínek chcete agenta MCA pokusit o zopakování operace MQPUT nebo MQOPEN. Určete název uživatelské procedury při definování kanálu.

2. vrátit odesilateli

   Pokud došlo k neúspěšnému pokusu o zopakování zprávy nebo byl zjištěn jiný typ chyby, může agent MCA odeslat zprávu zpět odesílateli. Chcete-li povolit vrácení odesilateli, je třeba při vkládání zprávy do původní fronty určit následující volby v deskriptoru zprávy:

   - Volba sestavy MQRO_EXCEPTION_WITH__FULL_DATA
   - Volba sestavy MQRO_DISCARD_MSG
   - Název fronty pro odpovědi a správce front pro odpovědi.

   Pokud program MCA nemůže vložit zprávu do cílové fronty, vygeneruje zprávu o výjimce obsahující původní zprávu a vloží ji do přenosové fronty, která má být odeslána do fronty pro odpovědi určené v původní zprávě. (Je-li fronta pro odpovědi ve stejném správci front jako MCA, zpráva se umístí přímo do této fronty, nikoli do přenosové fronty.)

3. Fronta nedoručených zpráv

   Pokud nelze zprávu doručit nebo vrátit, bude vložena do fronty nedoručených zpráv (DLQ). Obslužnou rutinu DLQ můžete použít ke zpracování zprávy. Toto zpracování je popsáno v tématu Zpracovávání zpráv ve frontě nedoručených zpráv pro systémy IBM MQ for UNIX, Linux a Windows a v Obslužném programu obslužné rutiny fronty nedoručených zpráv (CSQUDLQH) pro systémy z/OS . Není-li fronta nedoručených zpráv k dispozici, odesílající agent MCA ponechá zprávu v přenosové frontě a kanál se zastaví. Na rychlém kanálu jsou přechodné zprávy, které nelze zapsat do fronty nedoručených zpráv, ztraceny.

   Pokud v systému IBM WebSphere MQ 7.0není definována žádná lokální fronta nedoručených zpráv, vzdálená fronta není k dispozici nebo je definována a neexistuje žádná vzdálená fronta nedoručených zpráv, kanál odesílatele přejde do fronty RETRY a zprávy jsou automaticky odvolány do přenosové fronty.

Související odkazy

Použít frontu nedoručených zpráv (USEDLQ)

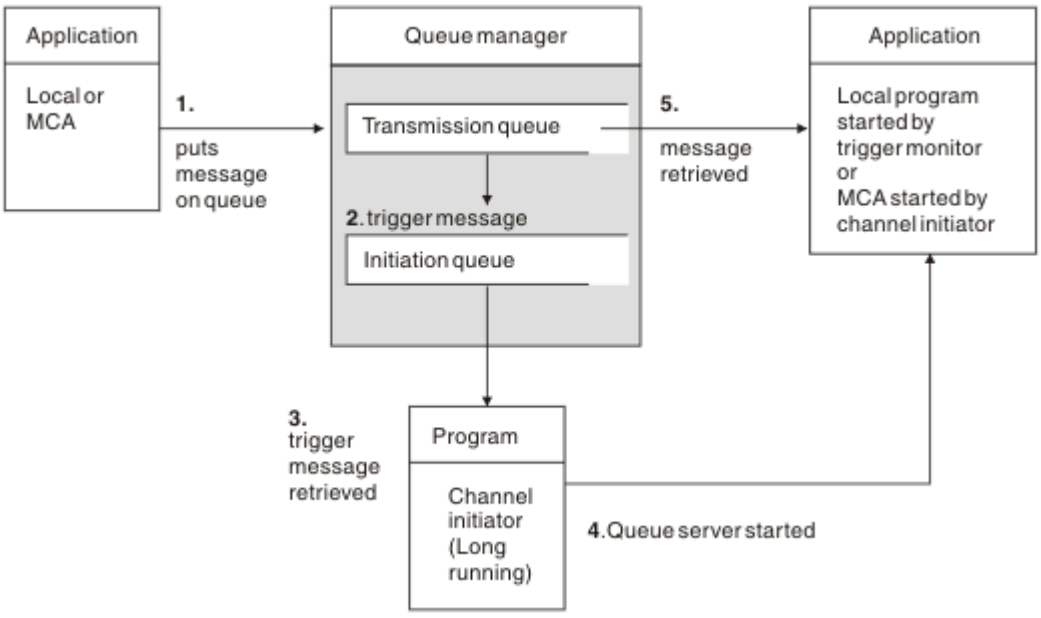
Spouštěcí kanály

Produkt IBM MQ poskytuje službu pro automatické spouštění aplikace, jsou-li splněny určité podmínky ve frontě. Toto zařízení se nazývá spouštění.

Toto vysvětlení je zamýšleno jako přehled spouštěcích koncepcí. Úplný popis naleznete v tématu Spuštění aplikací produktu IBM MQ pomocí spouštěčů.

Informace specifické pro danou platformu naleznete v následujících tématech:

- Pro produkt Windowsviz systémy UNIX and Linux , “Spouštění kanálů v systému UNIX, Linux, and Windows.” na stránce 215
- IBM i Pro IBM iviz “Spouštění kanálů v produktu IBM MQ for IBM i” na stránce 215
- z/OS Pro z/OSviz “Přenosové fronty a spouštěcí kanály” na stránce 874



Obrázek 26. Koncepty spouštění

Objekty požadované pro spuštění jsou zobrazeny v Obrázek 26 na stránce 214. Zobrazuje následující posloupnost událostí:

1. Lokální správce front umístí zprávu z aplikace nebo z agenta kanálu zpráv (MCA) v přenosové frontě.
2. Když jsou splněny spouštěcí podmínky, umístí lokální správce front zprávu spouštěče do inicializační fronty.
3. Inicializátor kanálu s dlouhou dobou zpracování monitoruje inicializační frontu a načítá zprávy tak, jak přicházejí.
4. Inicializátor kanálu zpracovává zprávy spouštěče podle informací obsažených v těchto zprávách. Tato informace může zahrnovat název kanálu, v tomto případě je spuštěna odpovídající agent MCA.
5. Lokální aplikace nebo agent MCA, který byl spuštěn, načítá zprávy z přenosové fronty.

Chcete-li nastavit tento scénář, musíte:

- Vytvořte přenosovou frontu s názvem inicializační fronty (to znamená SYSTEM.CHANNEL.INITQ) v odpovídajícím atributu.
- Ujistěte se, že je inicializační fronta (SYSTEM.CHANNEL.INITQ) existuje.
- Ujistěte se, že program inicializátoru kanálu je k dispozici a že je spuštěn. Program inicializátoru kanálu musí být zadán spolu s názvem inicializační fronty ve svém počátečním příkazu. z/OS V systému z/OSje název inicializační fronty opraven, takže není použit v příkazu ke spuštění.
- Volitelně vytvořte definici procesu pro spuštění, pokud neexistuje, a ujistěte se, že pole *UserData* obsahuje název kanálu, který obsluhuje. Místo vytvoření definice procesu můžete zadat název kanálu v atributu **TriggerData** přenosové fronty. IBM MQ pro systémy IBM i IBM i, UNIX, Linux, and Windows umožňuje, aby byl název kanálu zadán jako prázdný. V takovém případě se použije první dostupná definice kanálu s touto přenosovou frontou.
- Ujistěte se, že definice přenosové fronty obsahuje název definice procesu, která má sloužit, (je-li to vhodné), jméno inicializační fronty a spouštěcí charakteristiky, které cítíte nejvíce vhodné. Řídicí atribut spouštěče umožňuje aktivaci spouštěče, nebo nemusí být, jak je nezbytné.

Poznámka:

1. Inicializátor kanálu pracuje jako monitorování 'spouštěče monitoru', který monitoruje inicializační frontu používanou ke spouštění kanálů.
2. Inicializační fronta a spouštěcí proces lze použít ke spuštění libovolného počtu kanálů.
3. Může být definován libovolný počet inicializačních front a procesů spouštěče.
4. Doporučuje se typ spouštěče FIRST, aby se zabránilo zahlcení systému s inicializacím kanálu.

Spouštění kanálů v systému UNIX, Linux, and Windows.

ULW

Můžete vytvořit definici procesu v produktu IBM MQ, definování procesů, které mají být spuštěny. Příkaz MQSC DEFINE PROCESS použijte k vytvoření definice procesu pojmenovává proces, který má být spuštěn při příchodu zpráv do přenosové fronty. Atribut USERDATA definice procesu obsahuje název kanálu, který je obsluhován přenosovou frontou.

Definujte lokální frontu (QM4), která uvádí, že zprávy triggeru se mají zapsat do inicializační fronty (IQ), aby se spustila aplikace, která spouští kanál (QM3.TO.QM4):

```
DEFINE QLOCAL(QM4) TRIGGER INITQ(SYSTEM.CHANNEL.INITQ) PROCESS(P1) USAGE(XMITQ)
```

Definujte aplikaci (proces P1), která má být spuštěna:

```
DEFINE PROCESS(P1) USERDATA(QM3.TO.QM4)
```

Případně u systémů IBM MQ for UNIX, Linux a Windows můžete eliminovat potřebu definice procesu zadáním názvu kanálu v atributu TRIGDATA přenosové fronty.

Definujte lokální frontu (QM4). Určete, že zprávy spouštěče mají být zapsány do výchozí inicializační fronty SYSTEM.CHANNEL.INITQ, chcete-li spustit aplikaci (proces P1), která spouští kanál (QM3.TO.QM4):

```
DEFINE QLOCAL(QM4) TRIGGER INITQ(SYSTEM.CHANNEL.INITQ)
USAGE(XMITQ) TRIGDATA(QM3.TO.QM4)
```

Pokud nezadáte název kanálu, bude inicializátor kanálu hledat v souborech definice kanálu, dokud nenajde kanál, který je přidružen k uvedené přenosové frontě.

Spouštění kanálů v produktu IBM MQ for IBM i

IBM i

Spouštění kanálů v produktu IBM MQ for IBM i je implementováno s procesem inicializátoru kanálu. Proces inicializátoru kanálu pro inicializační frontu SYSTEM.CHANNEL.INITQ se spustí automaticky se správcem front, pokud není zakázán změnou atributu SCHINIT správce front.

Nastavte přenosovou frontu pro kanál tak, že uvedete SYSTEM.CHANNEL.INITQ jako inicializační frontu a povolení spouštění pro frontu. Inicializátor kanálu spustí první dostupný kanál, který uvádí tuto přenosovou frontu.

```
CRTMQMQ QNAME(MYXMITQ1) QTYPE(*LCL) MQMNAME(MYQMGR)
TRGENBL(*YES) INITQNAME(SYSTEM.CHANNEL.INITQ)
USAGE(*TMQ)
```

Můžete manuálně spustit až tři procesy inicializátoru kanálu s příkazem STRMQMCHLI a uvést různé inicializační fronty. Můžete také zadat více než jeden kanál, který dokáže zpracovat přenosovou frontu, a zvolit, který kanál se má spustit. Tato schopnost je stále poskytována jako kompatibilní se staršími verzemi. Jeho použití je zamítnuté.

Poznámka: Pouze jeden kanál v daném okamžiku může zpracovávat přenosovou frontu.

```
STRMQMCHLI QNAME(MYINITQ)
```

Nastavte přenosovou frontu pro kanál zadáním parametru TRGENBL (*YES) a výběrem kanálu, který se má pokusit o spuštění, určete název kanálu v poli TRIGDATA. Příklad:

```
CRTMQMQ QNAME(MYXMITQ2) QTYPE(*LCL) MQMNAME(MYQMGR)
TRGENBL(*YES) INITQNAME(MYINITQ)
USAGE(*TMQ) TRIGDATA(MYCHANNEL)
```

Související pojmy

"Spuštění a zastavení inicializátoru kanálu" na stránce 216

Spouštěcí impuls je implementován pomocí procesu inicializátoru kanálu.

Související úlohy

"Konfigurace distribuovaných front" na stránce 171

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související odkazy

Kanálové programy v systému UNIX, Linux, and Windows

IBM i Interkomunikační úlohy v systému IBM i

IBM i Stav kanálů v systému IBM i

Spuštění a zastavení inicializátoru kanálu

Spouštěcí impuls je implementován pomocí procesu inicializátoru kanálu.

Tento proces inicializátoru kanálu je spuštěn s příkazem MQSC START CHINIT. Pokud nepoužíváte výchozí inicializační frontu, zadejte do příkazu název inicializační fronty. Chcete-li například použít příkaz START CHINIT ke spuštění fronty IQ pro výchozího správce front, zadejte:

```
START CHINIT INITQ(IQ)
```

Ve výchozím nastavení je inicializátor kanálu spuštěn automaticky s použitím výchozí inicializační fronty SYSTEM.CHANNEL.INITQ. Chcete-li spustit všechny inicializátory kanálu ručně, postupujte takto:

1. Vytvořte a spusťte správce front.
2. Změnit vlastnost SCHINIT správce front na hodnotu MANUAL.
3. Ukončete a znovu spusťte správce front.

V systému IBM MQ for Multiplatforms je inicializátor kanálu spuštěn automaticky. Počet inicializátorů kanálu, které lze spustit, je omezen. Výchozí a současně maximální hodnota je 3. Tuto hodnotu můžete změnit pomocí parametru MAXINITIATORS v souboru qm.ini pro systémy UNIX and Linux a v registru pro systémy Windows .

Podrobnosti o příkazu spuštění inicializátoru kanálu **runmqchi**a o dalších řídicích příkazech najdete v tématu Řídicí příkazy produktu IBM MQ .

Zastavení inicializátoru kanálu

Výchozí inicializátor kanálu je spuštěn automaticky při spuštění správce front. Všechny inicializátory kanálu jsou automaticky zastaveny, pokud je správce front zastaven.

Inicializační a konfigurační soubory

Způsob zpracování inicializačních dat kanálu závisí na platformě IBM MQ .

z/OS systémy

z/OS

V produktu IBM MQ for z/OSjsou informace o inicializaci a konfiguraci zadány pomocí příkazu **ALTER QMGR** MQSC. Pokud vložíte **ALTER QMGR** příkazy do vstupní datové sady inicializace CSQINP2 , budou zpracovány při každém spuštění správce front.

Chcete-li spustit příkazy MQSC, jako je například **START LISTENER** při každém spuštění inicializátoru kanálu, vložte je do vstupní datové sady inicializace CSQINPX a zadejte do procedury spuštění úlohy iniciátoru kanálu nepovinný příkaz DD CSQINPX.

Další informace o souborech CSQINP2 a CSQINPX naleznete v tématu Úprava vstupních datových sad inicializacea ALTER QMGR.

Systémy Windows, IBM i, UNIX and Linux

V systémech IBM MQ for Windows, IBM i, UNIX and Linux jsou k dispozici konfigurační soubory pro uložení základních informací o konfiguraci instalace produktu IBM MQ .

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

IBM MQ konfigurační soubor
Tento soubor obsahuje informace vztahující se ke všem správcům front v systému IBM MQ . Tento soubor se nazývá `mqs.ini`. Je popsán v příručce “IBM MQ konfigurační soubor mqs.ini” na stránce 82.

Konfigurační soubor správce front

Tento soubor obsahuje informace o konfiguraci týkající se jednoho konkrétního správce front. Tento soubor se nazývá `qm.ini`.

Vytvoří se během vytváření správce front a může uchovávat informace o konfiguraci odpovídající libovolnému aspektu správce front. Informace obsažené v souboru obsahují podrobnosti o tom, jak se konfigurace protokolu liší od výchozí konfigurace v konfiguračním souboru IBM MQ .

Konfigurační soubor správce front je umístěn v kořenovém adresáři stromu adresáře obsazeného správcem front. Například pro atributy DefaultPath budou konfigurační soubory správce front pro správce front s názvem QMNAME vypadat takto:

Pro systémy UNIX and Linux :

```
/var/mqm/qmgrs/QMNAME/qm.ini
```

Následuje výňatek souboru `qm.ini` . Určuje, že modul listener protokolu TCP/IP má naslouchat na portu 2500, maximální počet aktuálních kanálů má být 200 a maximální počet aktivních kanálů musí být 100.

```
TCP:
Port=2500
CHANNELS:
MaxChannels=200
MaxActiveChannels=100
```

Můžete zadat rozsah portů TCP/IP, které má být použit pro odchozí kanál. Jednou z metod je použití souboru qm.ini k určení začátku a konce rozsahu hodnot portů. Následující příklad ukazuje soubor qm.ini s uvedením rozsahu kanálů:

```
TCP:
StrPort=2500
EndPort=3000
CHANNELS:
```

```
MaxChannels=200
MaxActiveChannels=100
```

Uvedete-li hodnotu pro StrPort nebo EndPort , musíte zadat hodnotu pro obě hodnoty. Hodnota parametru EndPort musí být vždy větší než hodnota parametru StrPort.

Kanál se pokusí použít každou z hodnot portů v určeném rozsahu. Když je připojení úspěšné, hodnota portu je port, který kanál poté použije.

Pro IBM i:

```
/QIBM/UserData/mqm/qmgrs/QMNAME/qm.ini
```

Pro systémy Windows :

```
C:\ProgramData\IBM\MQ\qmgrs\QMNAME\qm.ini
```

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

Převod dat 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:

- Řízení informací v deskriptoru zpráv
- Data aplikace

Obě části mohou vyžadovat konverzi dat, jsou-li odeslány mezi frontami v různých správcích front. Další informace o převodu dat aplikací naleznete v tématu Převod dat aplikací.

Psaní vlastních agentů kanálů zpráv

IBM MQ vám umožňuje zapsat si vlastní programy MCA (Message Channel Agent) nebo instalovat jeden z nezávislých dodavatelů softwaru.

Je možné, že budete chtít napsat své vlastní programy MCA, aby produkt IBM MQ pracoval nad vaším vlastním interním komunikačním protokolem nebo aby odesílal zprávy prostřednictvím protokolu, který produkt IBM MQ nepodporuje. (Chcete-li spolupracovat s agentem MCA pro práci s produktem IBM MQna druhém konci, nelze zapsat vlastní program MCA.)

Pokud se rozhodnete použít agenta MCA, který nebyl dodán produktem IBM MQ, je třeba vzít v úvahu následující body.

Odeslání a příjem zprávy
Musíte napsat odesílající aplikaci, která bude přijímat zprávy z místa, kde je aplikace uvede, například z přenosové fronty, a odešle je na protokol, se kterým chcete komunikovat. Musíte také napsat přijímající aplikaci, která přijímá zprávy z tohoto protokolu a vkládá je do cílových front. Odesílající a přijímající aplikace používají volání rozhraní fronty zpráv (MQI), nikoli žádná speciální rozhraní.

Musíte zajistit, aby zprávy byly doručeny pouze jednou. Koordinace bodů synchronizace může být použita k pomoci s tímto doručením.

Řídicí funkce kanálu
Chcete-li řídit kanály, musíte zadat své vlastní administrativní funkce. Administrační funkce kanálu produktu IBM MQ nelze použít pro konfiguraci (například příkaz DEFINE CHANNEL) nebo pro monitorování (například DISPLAY CHSTATUS) kanály.

Inicializační soubor
Pokud vyžadujete vlastní inicializační soubor, musíte zadat vlastní soubor inicializace.

Převod dat aplikace
Pravděpodobně budete chtít povolit konverzi dat pro zprávy, které posíláte do jiného systému. Je-li tomu tak, použijte volbu MQGMO_CONVERT při volání MQGET při načítání zpráv z libovolného místa, kde je aplikace umisťuje, například k přenosové frontě.

Uživatelské procedury
Zvažte, zda nepotřebujete uživatelské procedury. Pokud ano, můžete použít stejné definice rozhraní, které produkt IBM MQ používá.

Spouštění
Pokud vaše aplikace umísťuje zprávy do přenosové fronty, můžete nastavit atributy přenosové fronty tak, aby odesílaná MCA byla spuštěna, když zprávy dorazí do fronty.

Inicializátor kanálu
Je možné, že budete muset zadat svůj vlastní iniciátor kanálu.

Další informace, které je třeba zvážit při správě distribuovaných front

Další témata, která je třeba zvážit při přípravě produktu IBM MQ pro distribuovanou správu front. Toto téma pokrývá frontu nedoručených zpráv, Fronty v použití, Rozšíření systému a programy uživatelských procedur a Spouštění kanálů a listenerů jako ověřené aplikace.

Nedoručená-fronta zpráv

Chcete-li zajistit, aby byly zpracovány zprávy přicházející do fronty nedoručených zpráv (známé také jako fronta nedoručených zpráv nebo DLQ), vytvořte program, který lze spustit nebo spustit v pravidelných intervalech pro zpracování těchto zpráv.

Linux UNIX Obslužná rutina DLQ je poskytována s produktem IBM MQ v systémech UNIX and Linux . Další informace najdete v tématu Ukázka obslužné rutiny DLQ, amqsdlq.

IBM i Další informace o produktu IBM MQ for IBM inaleznete v tématu Obslužná rutina fronty nedoručených zpráv produktu IBM MQ for IBM i.

Fronty se používají

MCAs pro přijímací kanály může udržet cílové fronty otevřené i v případě, že zprávy nejsou přenášeny. Tyto výsledky ve frontách se zobrazují jako "v použití".

Maximální počet kanálů

IBM i V IBM MQ for IBM i můžete uvést maximální počet kanálů povolených ve vašem systému a maximální počet kanálů, které mohou být aktivní najednou. Tato čísla zadejte do souboru `qm.ini` v adresáři QIBM/UserData/mqm/qmgrs/*queue_manager_name*. Viz Stanzy konfiguračního souboru pro distribuované ukládání do fronty.

Rozšíření systému a programy uživatelské procedury

V definici kanálu je k dispozici zařízení, které umožňuje spouštění dalších programů v definovaných časech během zpracování zpráv. Tyto programy nejsou dodávány s produktem IBM MQ, ale lze je poskytovat každou instalací v souladu s místními požadavky.

Mají-li být tyto uživatelské programy spuštěny, musí mít předem definované názvy a musí být dostupné pro volání programů kanálu. Názvy programů uživatelských procedur jsou obsaženy v definicích kanálů zpráv.

Existuje definované řídicí blokovací rozhraní pro předání řízení těmto programům a pro manipulaci s návratem řízení z těchto programů.

Přesná místa, kde jsou tyto programy volány, a podrobnosti o řídicích blocích a názvech, najdete v tématu Programy výstupních bodů kanálů pro kanály systému zpráv.

Spuštění kanálů a listenerů jako důvěryhodných aplikací

Je-li výkon důležitým aspektem ve vašem prostředí a vaše prostředí je stabilní, můžete kanály a moduly listener spouštět jako důvěryhodné s použitím vazby FASTPATH. Existují dva faktory, které ovlivňují, zda jsou kanály a listenery spuštěny jako důvěryhodné:

- Proměnná prostředí MQ_CONNECT_TYPE=FASTPATH nebo MQ_CONNECT_TYPE = STANDARD. Rozlišují se malá a velká písmena. Uvedete-li hodnotu, která není platná, je ignorována.
- MQIBindType ve stanze Channels v souboru `qm.ini` nebo v souboru registru. Můžete jej nastavit na hodnotu FASTPATH nebo STANDARD a nerozlišují se malá a velká písmena. Výchozí hodnota je STANDARD.

Parametr MQIBindType můžete použít ve spojení s proměnnou prostředí k dosažení požadovaného účinku následujícím způsobem:

MQIBindType	Proměnná prostředí	Výsledek
STANDARD	Nedefinovaný	STANDARD
Rychlý	Nedefinovaný	Rychlý
STANDARD	STANDARD	STANDARD
Rychlý	STANDARD	STANDARD
STANDARD	Rychlý	STANDARD
Rychlý	Rychlý	Rychlý
STANDARD	CLIENT	CLIENT
Rychlý	CLIENT	STANDARD
STANDARD	LOCAL	STANDARD
Rychlý	LOCAL	STANDARD

V souhrnu existují pouze dva způsoby, jak lze kanály a listenery spustit jako důvěryhodné:

1. Uvedením parametru MQIBindType= FASTPATH v produktu `qm.ini` nebo v registru a neurčujete proměnnou prostředí.
2. Zadáním parametru MQIBindType= FASTPATH v produktu `qm.ini` nebo do registru a nastavením proměnné prostředí na hodnotu FASTPATH.

Zvažte spuštění listenerů jako důvěryhodných, protože listenery jsou stabilní procesy. Pokud nepoužíváte nestálý kanál nebo příkaz STOP CHANNEL MODE (TERMINATE), zvažte spuštění kanálů jako důvěryhodnosti.

ULW Monitorování a řízení kanálů v systému UNIX, Linux, and Windows

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

Informace o této úloze

Pro ovládání kanálů můžete použít následující typy příkazů:

Příkazy IBM MQ (MQSC)
Prostředí MQSC můžete použít jako jednotlivé příkazy v relaci MQSC v systémech UNIX, Linux, and Windows . Chcete-li vydat více komplikovaných nebo více příkazů, můžete prostředí MQSC sestavit do souboru, který lze poté spustit z příkazového řádku. Další informace najdete v tématu Příkazy MQSC. Tento oddíl uvádí některé jednoduché příklady použití MQSC pro distribuované fronty.

Příkazy kanálu jsou podmnožinou příkazů IBM MQ (MQSC). Použijte MQSC a řídicí příkazy pro:

- Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálu
- Spuštění a zastavení kanálů, testování spojení, resetování pořadových čísel kanálů a řešení sporných zpráv, pokud nelze znovu zavést propojení
- Zobrazení informací o stavu kanálů

Řídicí příkazy
Pro některé z těchto funkcí můžete také zadat příkaz *control commands* na příkazovém řádku. Podrobnosti najdete v tématu Administrace pomocí řídicích příkazů.

Formátovací příkazy Programovatelného příkazu
Podrobnosti naleznete v tématu Příkazy PCF.

Windows Linux **IBM MQ Explorer**
V systémech Linux a Windows můžete použít produkt IBM MQ Explorer. To poskytuje grafické rozhraní administrace pro provádění administrativních úloh jako alternativu k použití řídicích příkazů nebo příkazů MQSC. Definice kanálů jsou drženy jako objekty správce front.

Každý správce front má komponentu DQM pro řízení propojení mezi kompatibilními vzdálenými správci front. Oblast úložiště obsahuje pořadová čísla a *logical unit of work (LUW)* identifikátorů. Ty se používají pro účely synchronizace kanálu.

Seznam funkcí, které jsou vám k dispozici při nastavování a řízení kanálů zpráv s použitím různých typů příkazů, viz Tabulka 22 na stránce 222.

Procedura

- “Funkce vyžadované pro nastavení a řízení kanálů” na stránce 221
- “Začínáme s objekty” na stránce 224
- “Nastavení komunikace v systému Windows” na stránce 230
- “Nastavení komunikace v systému UNIX and Linux” na stránce 237

Související úlohy
“Monitorování a řízení kanálů v systému IBM i” na stránce 244
Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

Související odkazy
ULW Kanálové programy v systému UNIX, Linux, and Windows
ULW Příklad plánování kanálů zpráv pro produkt UNIX, Linux, and Windows
Příklad konfiguračních informací
Atributy kanálu

ULW Funkce vyžadované pro nastavení a řízení kanálů

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

Definici kanálu můžete vytvořit s použitím výchozích hodnot dodaných produktem IBM MQa s určením názvu kanálu, typu vytvářeného kanálu, metody komunikace, která má být použita, název přenosové fronty a název připojení.

Název kanálu musí být stejný na obou koncích kanálu a musí být jedinečný v rámci sítě. Musíte však omezit použité znaky na ty znaky, které jsou platné pro názvy objektů produktu IBM MQ .

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

- “Začínáme s objekty” na stránce 224
- “Vytváření přidružených objektů” na stránce 224
- “Vytváření výchozích objektů” na stránce 224

- “Vytvoření kanálu” na stránce 225
- “Zobrazení kanálu” na stránce 225
- “Zobrazení stavu kanálu” na stránce 226
- “Kontrola odkazů pomocí příkazu ping” na stránce 226
- “Spuštění kanálu” na stránce 226
- “Zastavení kanálu” na stránce 228
- “Přejmenování kanálu” na stránce 229
- “Resetování kanálu” na stránce 229
- “Vyřešení nejistých zpráv na kanálu” na stránce 229

Produkt Tabulka 22 na stránce 222 zobrazí úplný seznam funkcí produktu IBM MQ , které můžete potřebovat.

Tabulka 22. Funkce vyžadované v systémech UNIX, Linux, and Windows

Funkce	**Řídicí příkazy**	**MQSC**	**Ekvivalent průzkumníka IBM MQ ?**
Funkce správce front			
Změnit správce front		ALTER QMGR	Ano
Vytvoření správce front	crtmqm		Ano
Odstranit správce front	dltmqm		Ano
Zobrazit správce front		ZOBRAZIT QMGR	Ano
Ukončení správce front	endmqm		Ano
Odeslat signál Ping pro správce front		PING QMGR	Ne
Spustit správce front	strmqm		Ano
Funkce příkazového serveru			
Zobrazit příkazový server	dspmqcsv		Ne
Ukončit příkazový server	endmqcsv		Ne
Spustit příkazový server	strmqcsv		Ne
Funkce fronty			
Změnit frontu		POZMĚNIT PŘÍKAZ QALIAS ALTER QLOCAL ALTER QMODEL ALTER QREMOTE Viz téma Fronty ALTER.	Ano
Vymazat frontu		CLEAR QLOCAL	Ano
Vytvořit frontu		DEFINE QALIAS DEFINE QLOCAL DEFINE QMODEL DEFINE QREMOTE Viz DEFINE queues.	Ano

Tabulka 22. Funkce vyžadované v systémech UNIX, Linux, and Windows (pokračování)			
Funkce	**Řídicí příkazy**	**MQSC**	**Ekvivalent průzkumníka IBM MQ ?**
Odstranit frontu		VÝMAZ QALIAS DELETE QLOCAL DELETE QMODEL DELETE QREMOTE Viz DELETE queues.	Ano
Zobrazit frontu		ZOBRAZIT FRONTU	Ano
funkce procesu			
Změnit proces		ZMĚNA PROCES	Ano
Vytvořit proces		DEFINOVAT PROCES	Ano
Odstranit proces		Odstranit proces	Ano
Zobrazit proces		ZOBRAZIT PROCES	Ano
Funkce kanálu			
Změnit kanál		ALTER CHANNEL	Ano
Vytvořit kanál		Definovat kanál	Ano
Odstranit kanál		Odstranit kanál	Ano
Zobrazit kanál		DISPLAY CHANNEL	Ano
Zobrazit stav kanálu		ZOBRAZIT STAV CHSTATUS	Ano
Ukončit kanál		Ukončit kanál	Ano
Odeslat signál Ping pro kanál		Odeslat signál Ping pro kanál	Ano
Resetovat kanál		Resetovat kanál	Ano
Vyřešit kanál		Vyřešit kanál	Ano
Spustit kanál	runmqchl	Spustit kanál	Ano
Spustit inicializátor kanálu	runmqchi	START CHINIT	Ne
Spustit modul listener [1]	runmqlsr	Spustit listener	Ne
Koncový modul listener	endmqlsr, pouze na následujících platformách: • AIX • Solaris • Windows Systémy Windows		Ne

Poznámka:

1. Modul listener může být spuštěn automaticky při spuštění správce front.

ULW Začínáme s objekty

Kanály musí být definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál. Tento oddíl ukazuje, jak.

Použijte příkazy IBM MQ (MQSC) nebo IBM MQ Explorer pro:

1. Definování kanálů zpráv a přidružených objektů
2. Monitorování a řízení kanálů zpráv

Je možné, že přidružené objekty, které budete potřebovat definovat, jsou:

- Přenosové fronty
- Definice vzdálených front
- Definice aliasů správce front
- Definice aliasů fronty odpovědí
- Odpovědi na lokální fronty
- Procesy pro spouštění (MCA)
- Definice kanálů zpráv

Před spuštěním kanálu musí být definován a dostupný konkrétní komunikační spoj pro každý kanál. Popis způsobu, jakým jsou definovány propojení LU 6.2, TCP/IP, NetBIOS, SPX a DECnet, najdete v příslušné komunikační příručce pro vaši instalaci. Viz také Příklad konfiguračních informací.

Další informace o vytváření a práci s objekty naleznete v následujících dílčích tématech:

ULW *Vytváření přidružených objektů*

Prostředí MQSC se používá k vytvoření přidružených objektů.

Pomocí MQSC vytvořte frontu a objekty aliasu: přenosové fronty, definice vzdálených front, definice aliasů správce front, definice alias fronty odpovědí a odpovědi na lokální fronty.

Rovněž vytvořte definice procesů pro spouštění (MCAs) podobným způsobem.

Příklad, jak vytvořit všechny požadované objekty, najdete v tématu Příklad plánování kanálů zpráv pro produkt UNIX, Linux, and Windows.

ULW *Vytváření výchozích objektů*

Výchozí objekty jsou vytvářeny automaticky při vytvoření správce front. Těmito objekty jsou fronty, kanály, definice procesu a fronty administrace. Jakmile jsou výchozí objekty vytvořeny, můžete je kdykoli nahradit spuštěním příkazu strmqm s volbou -c.

Použijete-li příkaz crtmqm k vytvoření správce front, příkaz také inicializuje program a vytvoří sadu výchozích objektů.

1. Každý výchozí objekt je vytvořen na oplátku. Program uchovává počet úspěšně definovaných objektů, počet existujících objektů a jejich nahrazení a počet neúspěšných pokusů o jejich provedení.
2. Program zobrazí výsledky pro vás, a pokud došlo k nějakým chybám, přesměrovává vás do příslušného protokolu chyb kvůli podrobnostem.

Po dokončení spuštění programu můžete pomocí příkazu strmqm spustit správce front.

Další informace o příkazech crtmqm a strmqm najdete v tématu Správa pomocí řídicích příkazů .

Změna výchozích objektů

Pokud zadáte volbu -c, správce front bude během vytváření objektů spuštěn dočasně a poté se znovu vypne. Při vydání příkazu strmqm s volbou -c se obnoví existující systémové objekty s výchozími

hodnotami (například atribut MCAUSER definice kanálu je nastaven na prázdné). Chcete-li spustit správce front, je třeba příkaz strmqm znovu použít bez volby -c.

Chcete-li změnit výchozí objekty, můžete vytvořit svou vlastní verzi starého souboru amqscoma.tst a upravit ji.

ULW *Vytvoření kanálu*

Vytvořte dvě definice kanálu, jeden na každém konci připojení. První definici kanálu vytvoříte v prvním správci front. Poté vytvořte druhou definici kanálu v druhém správci front na druhém konci odkazu.

Oba konce musí být definovány pomocí stejného názvu kanálu. Dva konce musí mít kompatibilní typy kanálů, například: Sender and Receiver.

Chcete-li vytvořit definici kanálu pro jeden konec odkazu, použijte příkaz MQSC DEFINE CHANNEL. Zahrňte název kanálu, typ kanálu pro tento konec připojení, název připojení, popis (je-li požadován), název přenosové fronty (je-li to požadováno) a přenosový protokol. Zahrňte také všechny ostatní atributy, které se mají lišit od výchozích hodnot systému pro požadovaný typ kanálu, pomocí informací, které jste shromáždili dříve.

Poskytli jste nápovědu při rozhodování o hodnotách atributů kanálu v části Atributy kanálu.

Poznámka: Doporučuje se, abyste všechny kanály ve vaší síti pojmenovali jedinečně. Začlenění názvů zdrojového a cílového správce front do názvu kanálu je dobrý způsob, jak to provést.

Příklad příkazu create channel

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) +
DESCR('Sender channel to QM2') +
CONNAME(QM2) TRPTYPE(TCP) XMITQ(QM2) CONVERT(YES)
```

Ve všech příkladech příkazu MQSC se příkaz zobrazí tak, jak je uveden v souboru příkazů, a jak je zadán v souboru UNIX, Linux, and Windows. Tyto dvě metody vypadají stejně, kromě toho, že chcete-li spustit příkaz interaktivně, musíte nejprve spustit relaci MQSC. Zadejte `runmqsc`, pro výchozího správce front nebo `runmqsc` *qmname* , kde *qmname* je název požadovaného správce front. Pak zadejte libovolný počet příkazů, jak je uvedeno v příkladech.

Pro přenositelnost omezte délku řádku svých příkazů na 72 znaků. Použijte znak zřetězení, +, jak je zobrazeno pro pokračování více než jednoho řádku:

- Windows V systému Windows použijte klávesu Ctrl-z k ukončení položky na příkazovém řádku.
- Linux UNIX V systému UNIX and Linuxpoužijte klávesu Ctrl-d.
- Případně v systému UNIX, Linux, and Windowspoužijte příkaz **end** .

ULW *Zobrazení kanálu*

Chcete-li zobrazit atributy kanálu, použijte příkaz MQSC DISPLAY CHANNEL.

Parametr ALL příkazu DISPLAY CHANNEL se standardně předpokládá, pokud nejsou požadovány žádné specifické atributy a uvedený název kanálu není generický.

Atributy jsou popsány v části Atributy kanálu.

Zobrazit příklady kanálů

```
DISPLAY CHANNEL(QM1.TO.QM2) TRPTYPE,CONVERT

DISPLAY CHANNEL(QM1.TO.*) TRPTYPE,CONVERT

DISPLAY CHANNEL(*) TRPTYPE,CONVERT

DISPLAY CHANNEL(QM1.TO.QMR34) ALL
```

ULW *Zobrazení stavu kanálu*

Použijte příkaz MQSC DISPLAY CHSTATUS uvedením názvu kanálu a toho, zda chcete aktuální stav kanálů nebo stav uložených informací.

ZOBRAZIT CHSTATUS se vztahuje na všechny kanály zpráv. Nevztahuje se na kanály MQI jiné než kanály připojení serveru.

Zobrazené informace zahrnují:

- Název kanálu
- Název komunikačního připojení
- Na nejistém stavu kanálu (je-li to vhodné)
- Poslední pořadové číslo
- Název přenosové fronty (je-li to vhodné)
- Identifikátor v nejistém stavu (je-li to vhodné)
- Poslední potvrzené pořadové číslo
- Identifikátor logické pracovní jednotky
- ID procesu
- Windows ID vlákna (pouze Windows)

Zobrazit příklady stavu kanálu

```
DISPLAY CHSTATUS(*) CURRENT
DISPLAY CHSTATUS(QM1.TO.*) SAVED
```

Uložený stav se neuplatní, dokud nebude na kanálu přenesena alespoň jedna dávka zpráv. Stav se také uloží, když je kanál zastaven (pomocí příkazu STOP CHL) a když je ukončen správce front.

ULW *Kontrola odkazů pomocí příkazu ping*

Použijte příkaz MQSC pro příkaz PING CHANNEL, chcete-li vyměnit zprávu s pevnou datovou zprávou se vzdáleným koncem.

Příkaz Ping poskytuje určitou jistotu supervizorovi systému, že je tento odkaz k dispozici a funkční.

Příkaz ping nezahrnuje použití přenosových front a cílových front. Používá definice kanálu, související komunikační linku a nastavení sítě. Lze ji použít pouze v případě, že kanál není momentálně aktivní.

Je k dispozici pouze pro kanály odesílatele, serveru a odesílatele klastru. Odpovídající kanál se spouští na vzdálené straně odkazu a provádí vyjednávání parametrů spuštění. Chyby jsou oznámeny normálně.

Výsledek výměny zpráv se zobrazí jako `Ping complete` nebo chybová zpráva.

Příkaz ping s LU 6.2

Je-li příkaz PING vyvolán, standardně se do přijímacího konce nepřenášejí žádné ID uživatele nebo heslo. Jsou-li požadovány ID uživatele a heslo, mohou být vytvořeny na začátku inicializace v definici kanálu. Je-li heslo zadáno do definice kanálu, je před uložením zašifrováno produktem IBM MQ . Je poté dešifrováno před proudícím konverzací v rámci konverzace.

ULW *Spuštění kanálu*

Použijte příkaz MQSC START CHANNEL pro kanály odesílatele, serveru a žadatele. Aby aplikace mohly vyměňovat zprávy, musíte spustit program listener pro příchozí připojení.

Příkaz START CHANNEL není nutný, pokud byl kanál nastaven s použitím spouštěče správce front.

Když je spuštěna, odesílající agent MCA přečte definice kanálu a otevře přenosovou frontu. Je vydána spouštěcí posloupnost kanálu, která vzdáleně spustí odpovídající MCA přijímače nebo kanálu serveru. Po spuštění budou procesy odesílatele a serveru čekat na zprávy přicházející do přenosové fronty a předávají je, jakmile dorazí.

Používáte-li spouštěcí nebo spouštěcí kanály jako podprocesy, ujistěte se, že je k dispozici inicializátor kanálu pro monitorování inicializační fronty. Inicializátor kanálu je standardně spuštěn jako součást správce front.

Avšak TCP a LU 6.2 poskytují další schopnosti:

- Linux UNIX Pro protokol TCP v systému UNIX and Linuxmůže být démon inetd konfigurován pro spuštění kanálu. inetd se spouští jako oddělený proces.
- Linux UNIX Pro LU 6.2 v UNIX and Linuxnakonfigurujte svůj produkt SNA pro spuštění procesu odpovídacího modulu LU 6.2 .
- Windows Pro LU 6.2 v Windowspomocí serveru SNA můžete ke spuštění kanálu použít program TpStart (obslužný program dodávaný se serverem SNA). TpStart se spustí jako oddělený proces.

Použití volby Start vždy způsobí, že se kanál resynchronizuje, je-li to nutné.

Aby bylo možné začít úspěšně:

- Definice kanálů, lokální a vzdálené, musí existovat. Pokud neexistuje vhodná definice kanálu pro přijímací kanál nebo kanál připojení serveru, vytvoří se automaticky, je-li kanál automaticky definován, automaticky. Viz Channel auto-definition exit program.
- Přenosová fronta musí existovat a nesmí ji používat žádné jiné kanály.
- MCAs, místní a vzdálený, musí existovat.
- Komunikační spojení musí být k dispozici.
- Správci front musí být spuštění, lokálními a vzdálenými.
- Kanál zpráv nesmí být již spuštěn.

Zobrazí se zpráva potvrzující, že požadavek na spuštění kanálu byl přijat. Pro potvrzení, že spouštěcí příkaz byl úspěšný, zkontrolujte záznam chyb nebo použijte DISPLAY CHSTATUS. Protokoly chyb jsou:

Windows **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 stále také zobrazí zpráva v protokolu událostí aplikace systému Windows .

Linux UNIX **UNIX and Linux**

/var/mqm/qmgrs/qmname/errors/AMQERR01.LOG (pro každého správce front s názvem qmname)

/var/mqm/qmgrs/@SYSTEM/errors/AMQERR01.LOG (pro obecné chyby)

V systému UNIX, Linux, and Windowspoužijte příkaz **runmqlsr** ke spuštění procesu modulu listener produktu IBM MQ . Při výchozím nastavení všechny příchozí požadavky na připojení kanálu způsobí spuštění modulu listener MCA jako podprocesy procesu amqrmppa.

```
runmqlsr -t tcp -m QM2
```

Pro odchozí připojení musíte kanál spustit jedním z následujících tří způsobů:

1. Použijte příkaz MQSC START CHANNEL a uveďte název kanálu, aby se kanál spustil jako proces nebo podproces, v závislosti na parametru MCATYPE. (Jsou-li kanály spouštěny jako podprocesy, jsou podprocesy iniciátoru kanálu.)

```
START CHANNEL(QM1.TO.QM2)
```

2. Pomocí příkazu runmqchl příkazu spusťte kanál jako proces.

```
runmqchl -c QM1.TO.QM2 -m QM1
```

3. Použijte inicializátor kanálu ke spuštění kanálu.

ULW ***Zastavení kanálu***

Použijte příkaz MQSC STOP CHANNEL, chcete-li požádat kanál o zastavení aktivity. Kanál nespustí novou dávku zpráv až do okamžiku, kdy operátor znovu spustí kanál.

Informace o restartování zastavených kanálů viz “Restartování zastavených kanálů” na stránce 210.

Tento příkaz lze zadat na kanál libovolného typu s výjimkou MQCHT_CLNTCONN.

Můžete vybrat typ zastavení, který vyžadujete:

Příklad příkazu pro zastavení

```
STOP CHANNEL(QM1.TO.QM2) MODE(QUIESCE)
```

Tento příkaz požaduje, aby se kanál zavřel spořádaným způsobem. Aktuální dávka zpráv je dokončena a procedura synchronizace se provádí s druhým koncem kanálu. Je-li kanál nečinný, tento příkaz neukončí přijímací kanál.

Příklad příkazu Stop force

```
STOP CHANNEL(QM1.TO.QM2) MODE(FORCE)
```

Tato volba ihned zastaví kanál, ale nezastavuje podproces nebo proces kanálu. Kanál nedokončí zpracování aktuální dávky zpráv, a proto může kanál v nejistém stavu opustit kanál. Obecně lze uvažovat o použití volby zastavení uvedení do klidového stavu.

Zastavit příklad ukončení

```
STOP CHANNEL(QM1.TO.QM2) MODE(TERMINATE)
```

Tato volba ihned zastaví kanál a ukončí vlákno nebo proces kanálu.

Zastavit (uvést do klidového stavu) příklad zastavení

```
STOP CHANNEL(QM1.TO.QM2) STATUS(STOPPED)
```

Tento příkaz neuvádí režim MODE, takže je výchozí nastavení MODE (QUIESCE). Požaduje, aby byl kanál zastaven, aby jej nebylo možné automaticky restartovat, ale musí být spuštěn ručně.

Příklad zastavení (uvedení do klidového stavu)

```
STOP CHANNEL(QM1.TO.QM2) STATUS(INACTIVE)
```

Tento příkaz neuvádí režim MODE, takže je výchozí nastavení MODE (QUIESCE). Požaduje, aby byl kanál deaktivován, aby se automaticky restartoval, je-li to nutné.

ULW *Přejmenování kanálu*

K přejmenování kanálu zpráv použijte MQSC.

Použijte MQSC pro provedení následujících kroků:

1. Použijte příkaz STOP CHANNEL k zastavení kanálu.
2. Použijte příkaz DEFINE CHANNEL k vytvoření duplicitní definice kanálu s novým názvem.
3. Použijte příkaz DISPLAY CHANNEL, chcete-li zkontrolovat, zda byla vytvořena správně.
4. Použijte příkaz DELETE CHANNEL k odstranění původní definice kanálu.

Pokud se rozhodnete přejmenovat kanál zpráv, nezapomeňte, že kanál má dvě definice kanálu, jeden na každém konci. Ujistěte se, že jste přejmenovali kanál na obou koncích současně.

ULW *Resetování kanálu*

Chcete-li změnit pořadové číslo zprávy, použijte příkaz MQSC RESET CHANNEL.

Příkaz RESET CHANNEL je k dispozici pro všechny kanály zpráv, ale nikoli pro kanály MQI (připojení klienta nebo připojení k serveru). První zpráva začíná novou posloupností při příštím spuštění kanálu.

Je-li příkaz zadán na odesílacím nebo serverovém kanálu, informuje druhou stranu o změně kanálu po restartování kanálu.

Související pojmy

“Začínáme s objekty” na stránce 224
Kanály musí být definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál. Tento oddíl ukazuje, jak.

“Řídicí funkce kanálu” na stránce 199
Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

Související úlohy

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související odkazy

Resetovat kanál

ULW *Vyřešení nejistých zpráv na kanálu*

Použijte příkaz MQSC RESOLVE CHANNEL, jsou-li zprávy zadrženy nejistou odesilatelem nebo serverem. Například, protože jeden konec odkazu byl ukončen a není zde žádná vyhlídka na obnovení.

Příkaz RESOLVE CHANNEL přijímá jeden ze dvou parametrů: BACKOUT nebo COMMIT. Funkce Backout obnovuje zprávy do přenosové fronty, zatímco operace Commit je vyřazuje.

Program kanálu se nepokusí o vytvoření relace s partnerem. Místo toho určí identifikátor logické jednotky práce (LUWID), který reprezentuje neověřené zprávy. Podle požadavku se pak vydává buď:

- BACKOUT pro obnovení zpráv do přenosové fronty; nebo
- COMMIT pro odstranění zpráv z přenosové fronty.

Aby bylo řešení úspěšné, postupujte takto:

- Kanál musí být neaktivní
- Kanál musí mít pochybnosti.
- Typ kanálu musí být odesilatel, server nebo odesílatel klastru.
- Definice lokálního kanálu musí existovat
- Lokální správce front musí být spuštěn.

Související pojmy

“Začínáme s objekty” na stránce 224
Kanály musí být definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál. Tento oddíl ukazuje, jak.

“Řídicí funkce kanálu” na stránce 199
Funkce řízení kanálů poskytuje zařízení pro definování, monitorování a řízení kanálů.

Související úlohy

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

Související odkazy

Vyřešit kanál

Windows Nastavení komunikace v systému Windows

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby to bylo úspěšné, připojení musí být definováno a dostupné. Tento oddíl vysvětluje, jak to provést pomocí formulářů komunikace, které jsou k dispozici pro systémy IBM MQ for Windows .

Než začnete

Může se stát, že vám pomůže se podívat na Příklad konfigurace- IBM MQ for Windows.

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Informace o této úloze

Při nastavení komunikace pro produkt IBM MQ v systému Windowsmůžete vybírat z následujících typů komunikace:

- TCP/IP
- LU 6.2
- NetBIOS

Procedura

- Informace o nastavení komunikace pro váš systém Windows naleznete v dílčím tématu pro zvolený typ komunikace:
  - “Definování připojení TCP na systému Windows” na stránce 231
  - “Definování připojení LU 6.2 na systému Windows” na stránce 233
  - “Definování připojení NetBIOS v systému Windows” na stránce 234

  Ne všechny funkce a zařízení produktu IBM MQ for Windows jsou dostupné v prostředích, která používají komunikační protokoly jiné než TCP/IP. Položka, která není k dispozici, je IBM MQ Explorer.

Související úlohy

“Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 220
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 oblastí úložiště pro informace o synchronizaci.

“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 v systému UNIX and Linux” na stránce 237
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby to bylo úspěšné, připojení musí být definováno a dostupné. Tento oddíl vysvětluje, jak to provést pomocí formulářů komunikace, které jsou k dispozici pro systémy IBM MQ for UNIX or Linux .

Související odkazy

“Který typ komunikace použít” na stránce 15
Různé platformy podporují různé komunikační protokoly. Výběr přenosového protokolu závisí na vaší kombinaci IBM MQ MQI client a platforem serverů.

Windows *Definování připojení TCP na systému Windows*

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

Než začnete

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Odesílání: Konec

Do pole Název připojení v definici kanálu zadejte název hostitele nebo adresu TCP cílového počítače.

Port, který se má připojit, je výchozí hodnota 1414. Číslo portu 1414 je přiřazeno oprávnění Internet Assigned Numbers Authority k IBM MQ.

Chcete-li použít jiné číslo portu než výchozí, zadejte jej do pole názvu připojení v definici objektu kanálu takto:

```
DEFINE CHANNEL('channel name') CHLTYPE(SDR) +
          TRPTYPE(TCP) +
          CONNAME('OS2ROG3(1822)') +
          XMITQ('XMitQ name') +
          REPLACE
```

kde OS2ROG3 je název DNS vzdáleného správce front a 1822 je požadovaný port. (Musí se jednat o port, na kterém naslouchá modul listener na přijímajícím konci.)

Spuštěný kanál musí být zastaven a restartován, aby se mohla změnit změna definice objektu kanálu.

Výchozí číslo portu můžete změnit tak, že jej zadáte v souboru `.ini` pro produkt IBM MQ for Windows:

```
TCP:
Port=1822
```

Poznámka: Chcete-li vybrat číslo portu TCP/IP, které se má použít, použije produkt IBM MQ první číslo portu, které nalezne, v následujícím pořadí:

1. Číslo portu explicitně určené v definici kanálu nebo v příkazovém řádku. Toto číslo umožňuje potlačení výchozího čísla portu pro kanál.
2. Atribut port uvedený ve stanze TCP souboru `.ini` . Toto číslo umožňuje přepsání výchozího čísla portu pro správce front.

3. Výchozí hodnota 1414. Toto je číslo přiřazené IBM MQ úřadem Internet Assigned Numbers Authority pro příchozí i odchozí připojení.

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

Příjem na TCP

Chcete-li spustit přijímací program kanálu, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Můžete použít modul listener produktu IBM MQ .

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu.

Chcete-li spustit přijímací program kanálu, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Můžete použít modul listener produktu IBM MQ .

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

Základní příklad použití příkazu **runmqlsr** :

```
runmqlsr -t tcp [-m QMNAME] [-p 1822]
```

Hranaté závorky označují volitelné parametry; QMNAME není vyžadováno pro výchozího správce front a číslo portu se nepožaduje, pokud používáte výchozí hodnotu (1414). Číslo portu nesmí být vyšší než 65535.

Poznámka: Chcete-li vybrat číslo portu TCP/IP, které se má použít, použije produkt IBM MQ první číslo portu, které nalezne, v následujícím pořadí:

1. Číslo portu explicitně určené v definici kanálu nebo v příkazovém řádku. Toto číslo umožňuje potlačení výchozího čísla portu pro kanál.
2. Atribut port uvedený ve stanze TCP souboru `.ini` . Toto číslo umožňuje přepsání výchozího čísla portu pro správce front.
3. Výchozí hodnota 1414. Toto je číslo přiřazené IBM MQ úřadem Internet Assigned Numbers Authority pro příchozí i odchozí připojení.

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu “Spuštění kanálů a listenerů jako důvěryhodných aplikací” na stránce 220. Informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

Použití volby TCP/IP SO_KEEPALIVE

Chcete-li použít volbu Windows SO_KEEPALIVE, musíte do svého registru přidat následující položku:

```
TCP:
KeepAlive=yes
```

Další informace o volbě SO_KEEPALIVE viz “Kontrola, zda je druhý konec kanálu stále k dispozici” na stránce 206.

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

Použití volby nevyřízených požadavků na modul listener TCP

V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

Viz “Použití volby seznamu požadavků na modul listener TCP v systému IBM MQ for Multiplatforms” na stránce 241 , kde získáte další informace, a specifickou hodnotu pro Windows.

Windows *Definování připojení LU 6.2 na systému Windows*

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

Po konfiguraci architektury SNA pokračujte následujícím způsobem.

Informace naleznete v následující tabulce.

Tabulka 23. Nastavení na lokálním systému Windows pro vzdálenou platformu správce front

Vzdálená platforma	**TPNAME**	**TPPATH.**
z/OS nebo MVS/ESA bez CICS	Totéž jako v příslušných vedlejších informacích o vzdáleném správci front.	-
z/OS nebo MVS/ESA pomocí CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-
IBM i	Stejné jako porovnávací hodnota v záznamu směrování v systému IBM i .	-
Systémy UNIX and Linux	Totéž jako v příslušných vedlejších informacích o vzdáleném správci front.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nezvolnitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

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

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

For the latest information about configuring AnyNet SNA over TCP/IP, see the following online IBM documentation: AnyNet SNA přes TCP/IP and Obsluha uzlu SNA.

Související pojmy

“Odeslání konce na LU 6.2 na Windows” na stránce 233
Vytvořte objekt strany CPI-C (symbolické místo určení) z administrativní aplikace produktu LU 6.2 , kterou používáte. Zadejte tento název do pole Název připojení v definici kanálu. Také vytvořte odkaz LU 6.2 na partnera.

“Příjem na LU 6.2 na Windows” na stránce 234
Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu.

Windows *Odeslání konce na LU 6.2 na Windows*

Vytvořte objekt strany CPI-C (symbolické místo určení) z administrativní aplikace produktu LU 6.2 , kterou používáte. Zadejte tento název do pole Název připojení v definici kanálu. Také vytvořte odkaz LU 6.2 na partnera.

V objektu strany CPI-C zadejte název partnerské LU na přijímajícím počítači, název TP a název režimu. Příklad:

```
Partner LU Name              OS2ROG2
```

```
Partner TP Name              recv
Mode Name                    #INTER
```

Windows *Příjem na LU 6.2 na Windows*

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu.

Chcete-li spustit přijímací program kanálu, musí být spuštěn program listener, který zjistí příchozí požadavky na síť a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu RUNMQLSR, zadáním příkazu TpName , na kterém bude naslouchat. Případně můžete pro produkt Windowspoužít TpStart pod serverem SNA Server.

Použití příkazu RUNMQLSR

Příklad příkazu pro spuštění modulu listener:

```
RUNMQLSR -t LU62 -n RECV [-m QMNAME]
```

kde RECV je TpName , který je zadán na druhém konci (odesílání) jako "TpName ke spuštění na vzdálené straně". Poslední část v hranatých závorkách je volitelná a není vyžadována pro výchozího správce front.

Je možné mít více než jednoho správce front spuštěného na jednom počítači. Každému správci front je třeba přiřadit různé položky TpName a poté pro každou z nich spustit program modulu listener. Příklad:

```
RUNMQLSR -t LU62 -m QM1 -n TpName1
RUNMQLSR -t LU62 -m QM2 -n TpName2
```

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu Spouštění kanálů a listenerů jako důvěryhodné aplikace. Informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

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

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

Použití serveru Microsoft SNA na systému Windows

Program TpSetup (ze sady SDK serveru SNA) můžete použít k definování vyvolaného TP, který pak vyvolá příkaz amqcrs6a.exe, nebo můžete ručně nastavit různé hodnoty registru. Parametry, které by měly být předány do souboru amqcrs6a.exe jsou:

```
-m QM -n TpName
```

kde *QM* je název správce front a *TpName* je název TP. Další informace naleznete v příručce *Microsoft SNA Server APPC Programmers Guide* nebo v příručce *Microsoft SNA Server CPI-C Programmers Guide* .

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

Windows *Definování připojení NetBIOS v systému Windows*

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

Každý běžící kanál, bez ohledu na typ, používá jednu relaci NetBIOS a jeden příkaz NetBIOS . Implementace NetBIOS produktu IBM umožňuje více procesům používat stejný lokální název NetBIOS . Proto musí být k dispozici pouze jeden název NetBIOS pro použití produktem IBM MQ. Implementace

jiných dodavatelů, například emulace NetBIOS společnosti Novell, vyžadují pro každý proces odlišný lokální název. Ověřte své požadavky z dokumentace k produktu NetBIOS , který používáte.

Ve všech případech se ujistěte, že jsou již k dispozici dostatečné prostředky pro každý typ, nebo zvyšte maximální hodnoty uvedené v konfiguraci. Jakékoli změny hodnot vyžadují restart systému.

Během spouštění systému zobrazuje ovladač zařízení NetBIOS počet relací, příkazů a názvů, které jsou k dispozici pro použití aplikacemi. Tyto prostředky jsou k dispozici pro každou aplikaci založenou na systému NetBIOS, která je spuštěna na stejném systému. Proto je možné, aby jiné aplikace spotřebovávají tyto prostředky dříve, než je produkt IBM MQ potřebuje získat. Administrátor sítě LAN by vám to měl být schopen objasnit.

Související pojmy

“Definování lokálního názvu NetBIOS produktu IBM MQ” na stránce 235
Lokální název NetBIOS používaný procesy kanálu produktu IBM MQ lze určit třemi způsoby.

“Vytváření omezení relací, příkazů a názvů správce front NetBIOS” na stránce 236
Omezení správce front pro relace NetBIOS , příkazy a názvy lze zadat dvěma způsoby.

“Zavedení čísla adaptéru LAN” na stránce 236
Aby kanály fungovaly úspěšně napříč protokolem NetBIOS, musí být podpora adaptéru na každém konci kompatibilní. Produkt IBM MQ umožňuje řídit výběr čísla adaptéru LAN (LANA) pomocí hodnoty AdapterNum v sekci NETBIOS vašeho souboru qm.ini a zadáním parametru **-a** v příkazu runmqlsr.

“Inicializace připojení NetBIOS” na stránce 236
Definování kroků potřebných k zahájení připojení.

“Definování cílového modulu listener pro připojení NetBIOS” na stránce 237
Definování kroků, které mají být provedeny na přijímajícím konci připojení NetBIOS .

Windows *Definování lokálního názvu NetBIOS produktu IBM MQ*

Lokální název NetBIOS používaný procesy kanálu produktu IBM MQ lze určit třemi způsoby.

V pořadí priorit jsou tyto tři způsoby:

1. Hodnota zadaná v parametru **-l** příkazu RUNMQLSR, například:

   ```
   RUNMQLSR -t NETBIOS -l my_station
   ```

2. Proměnná prostředí MQNAME s hodnotou, která je vytvořena příkazem:

   ```
   SET MQNAME= my_station
   ```

   Pro každý proces můžete nastavit hodnotu MQNAME. Případně je můžete nastavit na úrovni systému v registru Windows .

   Používáte-li implementaci NetBIOS , která vyžaduje jedinečné názvy, musíte v každém okně, ve kterém je spuštěn proces IBM MQ , zadat příkaz SET MQNAME. Hodnota MQNAME je libovolná, ale musí být jedinečná pro každý proces.

3. Oddíl NETBIOS v konfiguračním souboru správce front qm.ini. Příklad:

   ```
   NETBIOS:
   LocalName= my_station
   ```

Poznámka:

1. Vzhledem k rozdílům v implementaci podporovaných produktů NetBIOS se doporučuje, aby se každý název NetBIOS každý v síti jedinečný. Pokud tak neuvidíte, může dojít k nepředvídatelným výsledkům. Pokud máte problémy se zavedením kanálu NetBIOS a v chybovém protokolu správce front jsou uvedeny chybové zprávy ukazující návratový kód NetBIOS X'15 ', zkontrolujte, zda používáte názvy NetBIOS .

2. V systému Windowsnelze použít název počítače jako název NetBIOS , protože jej produkt Windows již používá.
3. Inicializace kanálu odesílatele vyžaduje, aby byl zadán název NetBIOS buď pomocí proměnné prostředí MQNAME, nebo pomocí proměnné LocalName v souboru qm.ini .

Windows *Vytváření omezení relací, příkazů a názvů správce front NetBIOS*

Omezení správce front pro relace NetBIOS , příkazy a názvy lze zadat dvěma způsoby.

V pořadí přednosti jsou tyto způsoby:

1. Hodnoty zadané v příkazu RUNMQLSR:

```
-s Sessions
-e Names
-o Commands
```

   Pokud v příkazu není zadán operand -m, použijí se hodnoty pouze pro výchozího správce front.
2. Oddíl NETBIOS v konfiguračním souboru správce front qm.ini. Příklad:

```
NETBIOS:

NumSess= Qmgr_max_sess
NumCmds= Qmgr_max_cmds
NumNames= Qmgr_max_names
```

Windows *Zavedení čísla adaptéru LAN*

Aby kanály fungovaly úspěšně napříč protokolem NetBIOS, musí být podpora adaptéru na každém konci kompatibilní. Produkt IBM MQ umožňuje řídit výběr čísla adaptéru LAN (LANA) pomocí hodnoty AdapterNum v sekci NETBIOS vašeho souboru qm.ini a zadáním parametru **-a** v příkazu runmqlsr.

Výchozí číslo adaptéru LAN použité produktem IBM MQ pro připojení NetBIOS je 0. Ověřte, jaké číslo se používá ve vašem systému, a to následujícím způsobem:

V systému Windowsnení možné zadávat dotazy na číslo adaptéru LAN přímo prostřednictvím operačního systému. Místo toho použijte LANACFG.EXE obslužný program příkazového řádku, dostupný z produktu Microsoft. Výstup nástroje zobrazuje čísla virtuálních adaptérů LAN a jejich účinné vazby. Další informace o číslech adaptérů LAN najdete v článku 138037 znalostní báze produktu Microsoft *HOWTO: Použití čísel LANA v 32bitovém prostředí*.

Určete správnou hodnotu v sekci NETBIOS konfiguračního souboru správce front qm.ini:

```
NETBIOS:
AdapterNum= n
```

kde n je správné číslo adaptéru LAN pro tento systém.

Windows *Inicializace připojení NetBIOS*

Definování kroků potřebných k zahájení připojení.

Chcete-li iniciovat připojení, proveďte následující kroky na odesílajícím konci:

1. Definujte název stanice NetBIOS pomocí hodnoty MQNAME nebo LocalName .
2. Ověřte, že číslo adaptéru LAN v systému je používáno, a zadejte správný soubor pomocí AdapterNum.
3. Do pole ConnectionName v definici kanálu zadejte název NetBIOS používaný cílovým programem modulu listener. V systému Windowsmusí být kanály NetBIOS spuštěny jako podprocesy. To lze provést zadáním parametru MCATYPE (THREAD) v definici kanálu.

```
DEFINE CHANNEL (chname) CHLTYPE(SDR) +
TRPTYPE(NETBIOS) +
CONNAME(your_station) +
```

```
XMITQ(xmitq) +
MCATYPE(THREAD) +
REPLACE
```

Windows *Definování cílového modulu listener pro připojení NetBIOS*

Definování kroků, které mají být provedeny na přijímajícím konci připojení NetBIOS .

Na přijímajícím konci proveďte následující kroky:

1. Definujte název stanice NetBIOS pomocí hodnoty MQNAME nebo LocalName .
2. Ověřte, že číslo adaptéru LAN v systému je používáno, a zadejte správný soubor pomocí AdapterNum.
3. Definujte přijímací kanál:

```
DEFINE CHANNEL (chname) CHLTYPE(RCVR) +
TRPTYPE(NETBIOS) +
REPLACE
```

4. Spuštěním programu modulu listener produktu IBM MQ vytvořte stanici a zpřístupníte ji tak, aby se s ní spojili. Příklad:

```
RUNMQLSR -t NETBIOS -l your_station [-m qmgr]
```

   Tento příkaz ustanoví `your_station` jako stanici NetBIOS čekající na kontaktování. Název stanice NetBIOS musí být jedinečný v rámci sítě NetBIOS .

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu “Spuštění kanálů a listenerů jako důvěryhodných aplikací” na stránce 220. Informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

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

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

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

Linux UNIX Nastavení komunikace v systému UNIX and Linux

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby to bylo úspěšné, připojení musí být definováno a dostupné. Tento oddíl vysvětluje, jak to provést pomocí formulářů komunikace, které jsou k dispozici pro systémy IBM MQ for UNIX or Linux .

Než začnete

Může se stát, že vám pomůže se podívat na následující oddíly:

- AIX Příklad konfigurace- IBM MQ for AIX
- Solaris Příklad konfigurace- IBM MQ for Solaris
- Linux Příklad konfigurace- IBM MQ pro Linux

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Informace o této úloze

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nutné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak to provést.

Při nastavení komunikace pro produkt IBM MQ v systému UNIX and Linuxmůžete vybírat z následujících typů komunikace:

- TCP/IP
- LU 6.2

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

Pro IBM MQ MQI clientsmůže být užitečné mít alternativní kanály používající různé přenosové protokoly. Další informace o produktu IBM MQ MQI clientsnaleznete v tématu Přehled produktu IBM MQ MQI clients.

Postup

Informace o nastavení komunikace pro váš systém UNIX and Linux naleznete v dílčím tématu pro zvolený typ komunikace:

- “Definování připojení TCP na systému UNIX and Linux” na stránce 238
- “Definování připojení LU 6.2 na systému UNIX and Linux” na stránce 242
- V 9.1.4 MQ Adv. Linux CD “Definování připojení Aspera gateway v systému Linux” na stránce 757

Související úlohy

“Monitorování a řízení kanálů v systému UNIX, Linux, and Windows” na stránce 220
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 oblastí úložiště pro informace o synchronizaci.

“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 v systému Windows” na stránce 230
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby to bylo úspěšné, připojení musí být definováno a dostupné. Tento oddíl vysvětluje, jak to provést pomocí formulářů komunikace, které jsou k dispozici pro systémy IBM MQ for Windows .

Související odkazy

“Který typ komunikace použít” na stránce 15
Různé platformy podporují různé komunikační protokoly. Výběr přenosového protokolu závisí na vaší kombinaci IBM MQ MQI client a platforem serverů.

Linux UNIX *Definování připojení TCP na systému UNIX and Linux*

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

Než začnete

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Odesílání: Konec

Do pole Název připojení v definici kanálu zadejte název hostitele nebo adresu TCP cílového počítače. Port, který se má připojit, je výchozí hodnota 1414. Číslo portu 1414 je přiřazeno oprávnění Internet Assigned Numbers Authority k IBM MQ.

Chcete-li použít jiné číslo portu než výchozí, změňte pole s názvem připojení takto:

```
Connection Name REMHOST(1822)
```

kde REMHOST je název uzlu vzdáleného počítače a 1822 je číslo portu, které se požaduje. (Musí se jednat o port, na kterém naslouchá modul listener na přijímajícím konci.)

Další možností je změnit číslo portu jeho určením v konfiguračním souboru správce front (qm.ini):

```
TCP:
Port=1822
```

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

Příjem na TCP

Můžete použít buď modul listener protokolu TCP/IP, který je démon inet (inetd), nebo modul listener produktu IBM MQ .

Některé distribuce Linux nyní používají rozšířený démon inet (xinetd) místo démona inet. Další informace o tom, jak používat rozšířený démon inet na systému Linux , najdete v tématu Ustanovení připojení TCP na systému Linux .

Související pojmy

“Použití modulu listener protokolu TCP/IP v systému UNIX and Linux” na stránce 239
Chcete-li spustit kanály v systému UNIX and Linux, je třeba upravit soubor `/etc/services` a soubor `inetd.conf` .

“Použití volby seznamu požadavků na modul listener TCP v systému IBM MQ for Multiplatforms” na stránce 241
V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

“Použití modulu listener produktu IBM MQ” na stránce 241
Chcete-li spustit modul listener dodávaný s produktem IBM MQ, který spouští nové kanály jako podprocesy, použijte příkaz `runmqlsr` .

“Použití volby TCP/IP SO_KEEPALIVE” na stránce 242
Na některých systémech UNIX and Linux můžete definovat, jak dlouho TCP čeká před kontrolou, zda je připojení stále dostupné, a jak často se znovu pokusí o připojení, pokud selže první kontrola. Je to buď laditelný parametr jádra, nebo jej lze zadat na příkazovém řádku.

Použití modulu listener protokolu TCP/IP v systému UNIX and Linux

Chcete-li spustit kanály v systému UNIX and Linux, je třeba upravit soubor `/etc/services` a soubor `inetd.conf` .

Postupujte podle těchto pokynů:

1. Upravte soubor `/etc/services` :

   Poznámka: Chcete-li upravit soubor `/etc/services` , musíte být přihlášeni jako uživatel root nebo root. Můžete to změnit, ale musí se shodovat s číslem portu uvedeným na konci odesílání.

Přidejte do souboru následující parametr:

```
MQSeries 1414/tcp
```

kde 1414 je číslo portu požadované produktem IBM MQ. Číslo portu nesmí být vyšší než 65535.

2. Přidejte řádek do souboru `inetd.conf`, chcete-li volat program amqcrsta, kde *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ :

```
MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta
[-m Queue_Man_Name]
```

Aktualizace jsou aktivní poté, co démon inetd znovu četl konfigurační soubory. Chcete-li to provést, zadejte následující příkazy z ID uživatele root:

- AIX V systému AIX:

```
refresh -s inetd
```

- Solaris V systémech Solaris 10 nebo novějších:

```
inetconv
```

- Linux UNIX Na jiných systémech UNIX and Linux (včetně Solaris 9):

```
kill -1 process_number
```

Když program listener spuštěný démonem inetd dědí národní prostředí z inetd, je možné, že prostředí MQMDE není dodrženo (sloučeno) a je umístěno do fronty jako data zprávy. Abyste se ujistili, že je prostředí MQMDE uznáno, musíte nastavit národní prostředí správně. Národní prostředí nastavené inetd se nemusí shodovat s národním prostředím vybraným pro jiná národní prostředí používaná procesy IBM MQ . Nastavení národního prostředí:

1. Vytvořte skript shellu, který nastaví proměnné prostředí proměnné prostředí LANG, LC_COLLATE, LC_CTYPE, LC_MONETARY, LC_NUMERIC, LC_TIME a LC_MESSAGES na národní prostředí použité pro další proces IBM MQ .
2. Ve stejném skriptu shellu zavolejte program modulu listener.
3. Upravte soubor `inetd.conf` tak, aby volal váš skript shellu místo programu modulu listener.

Na serveru je možné mít více než jednoho správce front. Do každého z těchto dvou souborů musíte přidat řádek pro každého správce front. Příklad:

```
MQSeries1   1414/tcp
MQSeries2   1822/tcp
```

```
MQSeries2 stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta -m QM2
```

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

Tím se vyvarujete generování chybových zpráv, pokud dojde k omezení počtu nevyřízených požadavků na připojení zařazených do fronty na jednom portu TCP. Informace o počtu neprovedených požadavků na připojení najdete v tématu “Použití volby seznamu požadavků na modul listener TCP v systému IBM MQ for Multiplatforms” na stránce 241.

Multi *Použití volby seznamu požadavků na modul listener TCP v systému IBM MQ for Multiplatforms*
V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

Výchozí hodnoty nevyřízených požadavků listeneru jsou zobrazeny v Tabulka 24 na stránce 241.

Tabulka 24. Maximální počet nevyřízených požadavků na připojení zařazených do fronty na portu TCP/IP

Platforma serveru	**Maximum požadavků na připojení**
AIX AIX	100
Linux Linux	100
IBM i IBM i	255
Solaris Solaris	100
Windows ServerWindows	100

Pokud se nahromadění nevyřízených požadavků dosáhne hodnot zobrazených v Tabulka 24 na stránce 241, připojení TCP/IP se odmítne a kanál se nebude moci spustit.

V případě kanálu MCA se tyto výsledky ve kanálu přejdou do stavu ZOPAKOVAT a znovu se pokusí o připojení později.

Chcete-li se však této chybě vyhnout, můžete přidat položku do souboru `qm.ini` :

```
TCP:
ListenerBacklog = n
```

Tento parametr přepíše výchozí maximální počet nevyřízených požadavků (viz Tabulka 24 na stránce 241). pro modul listener protokolu TCP/IP.

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí. V případě potřeby lze tuto hodnotu použít, abyste se vyhnuli dosažení limitu připojení.

Chcete-li spustit modul listener s 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`** naleznete v části runmqlsr. Další informace o příkazu DEFINE LISTENER naleznete v tématu DEFINE LISTENER.

Související pojmy

“Použití volby nevyřízených požadavků na modul listener TCP” na stránce 894
Při příjmu v protokolu TCP/IP je nastaven maximální počet neprovedených požadavků na připojení. Tyto nevyřízené požadavky mohou být považovány za *nevyřízené požadavky* požadavků čekajících na portu TCP/IP pro modul listener, aby přijal požadavek.

Linux UNIX *Použití modulu listener produktu IBM MQ*
Chcete-li spustit modul listener dodávaný 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; QMNAME není vyžadováno pro výchozího správce front a číslo portu se nepožaduje, pokud používáte výchozí hodnotu (1414). Číslo portu nesmí být vyšší než 65535.

Chcete-li dosáhnout nejlepšího výkonu, spusťte modul listener produktu IBM MQ jako důvěryhodnou aplikaci, jak je popsáno v tématu “Spuštění kanálů a listenerů jako důvěryhodných aplikací” na stránce 220. Informace o důvěryhodných aplikacích najdete v tématu Omezení pro důvěryhodné aplikace .

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

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

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

Linux UNIX *Použití volby TCP/IP SO_KEEPALIVE*

Na některých systémech UNIX and Linux můžete definovat, jak dlouho TCP čeká před kontrolou, zda je připojení stále dostupné, a jak často se znovu pokusí o připojení, pokud selže první kontrola. Je to buď laditelný parametr jádra, nebo jej lze zadat na příkazovém řádku.

Chcete-li použít volbu SO_KEEPALIVE (další informace viz “Kontrola, zda je druhý konec kanálu stále k dispozici” na stránce 206) Do konfiguračního souboru správce front (qm.ini) je třeba přidat následující položku:

```
TCP:
KeepAlive=yes
```

Další informace naleznete v dokumentaci k systému UNIX and Linux .

Linux UNIX *Definování připojení LU 6.2 na systému UNIX and Linux*

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

Nejnovější informace o konfiguraci SNA přes TCP/IP najdete v následující online dokumentaci IBM : Communications Server.

Musí být konfigurována služba SNA, aby bylo možné navázat konverzaci s LU 6.2 mezi dvěma systémy.

Informace naleznete v příručce *Multiplatform APPC Configuration Guide* a v následující tabulce.

Tabulka 25. Nastavení na lokálním systému UNIX and Linux pro vzdálenou platformu správce front

Vzdálená platforma	**TPNAME**	**TPPATH.**
z/OS bez CICS	Stejné jako odpovídající TPName v informacích o připojení vzdáleného správce front.	-
z/OS použití CICS	CKRC (odesílatel) CKSV (žadatel) CKRC (server)	-
IBM i	Stejné jako porovnávací hodnota v záznamu směrování v systému IBM i .	-
Systémy UNIX and Linux	Stejné jako odpovídající TPName v informacích o připojení vzdáleného správce front.	*MQ_INSTALLATION_PATH*/bin/amqcrs6a

Tabulka 25. Nastavení na lokálním systému UNIX and Linux pro vzdálenou platformu správce front (pokračování)		
Vzdálená platforma	**TPNAME**	**TPPATH.**
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nezvolnitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.	*MQ_INSTALLATION_PATH*\bin\amqcrs6a

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

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

Související pojmy

“Odeslání konce na LU 6.2 na UNIX and Linux” na stránce 243
V systému UNIX and Linux vytvořte objekt strany CPI-C (symbolické místo určení) a do pole Název připojení v definici kanálu zadejte tento název. Také vytvořte odkaz LU 6.2 na partnera.

“Příjem na LU 6.2 na UNIX and Linux” na stránce 243
Na systémech UNIX and Linux vytvořte naslouchací přílohu na přijímajícím konci, profil logické připojení LU 6.2 a profil TPN.

Linux UNIX *Odeslání konce na LU 6.2 na UNIX and Linux*

V systému UNIX and Linux vytvořte objekt strany CPI-C (symbolické místo určení) a do pole Název připojení v definici kanálu zadejte tento název. Také vytvořte odkaz LU 6.2 na partnera.

V bočním objektu CPI-C zadejte název partnerské LU na přijímajícím počítači, název transakčního programu a název režimu. Příklad:

```
Partner LU Name              REMHOST
Remote TP Name               recv
Service Transaction Program  no
Mode Name                    #INTER
```

Solaris V systému Solarisnastavte proměnnou prostředí APPC_LOCAL_LU na název lokální LU.

SECURITY PROGRAM se používá, je-li podporován CPI-C, když se IBM MQ pokusí o zavedení relace SNA.

Linux UNIX *Příjem na LU 6.2 na UNIX and Linux*

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

V profilu TPN zadejte úplnou cestu ke spustitelnému souboru a k názvu transakčního programu:

```
Full path to TPN executable    MQ_INSTALLATION_PATH/bin/amqcrs6a
Transaction Program name      recv
User ID                       0
```

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

V systémech, kde můžete nastavit ID uživatele, zadejte uživatele, který je členem skupiny mqm.

Solaris AIX V systémech AIXa Solarisnastavte proměnné prostředí APPCTPN (název transakce) a APPCLLU (lokální LU) (můžete použít konfigurační panely pro vyvolaný transakční program).

Možná bude třeba použít jiného správce front, než je výchozí správce front. Pokud ano, definujte příkazový soubor, který volá:

```
amqcrs6a -m Queue_Man_Name
```

a pak zavolejte do příkazového souboru.

IBM i Monitorování a řízení kanálů v systému IBM i

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

Informace o této úloze

Následující seznam je stručným popisem komponent funkce řízení kanálů:

- Definice kanálů jsou drženy jako objekty správce front.
- Příkazy kanálu jsou podmnožinou sady příkazů IBM MQ for IBM i .

  Použijte příkaz GO CMDMQM k zobrazení úplné sady příkazů IBM MQ for IBM i .
- Použijte panely definice kanálu nebo příkazy pro:
  - Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálu
  - Spuštění a zastavení kanálů, testování spojení, resetování pořadových čísel kanálů a řešení sporných zpráv, pokud nelze znovu zavést propojení
  - Zobrazení informací o stavu kanálů
- Kanály lze také spravovat pomocí prostředí MQSC.
- Kanály lze také spravovat pomocí Průzkumníka IBM MQ
- Pořadová čísla a identifikátory *logické pracovní jednotky (LUW)* jsou uloženy v souboru synchronizace a používají se pro účely synchronizace kanálů.

Příkazy a panely můžete použít k definování kanálů zpráv a přidružených objektů a monitorování a řízení kanálů zpráv. Pomocí klávesy F4=Prompt můžete uvést odpovídajícího správce front. Pokud nepoužijete výzvu k zadání, předpokládá se výchozí správce front. S klávesou F4=Promptse zobrazí další panel, na kterém můžete zadat příslušný název správce front a někdy i další data.

Objekty, které potřebujete definovat s panely, jsou:

- Přenosové fronty
- Definice vzdálených front
- Definice aliasů správce front
- Definice aliasů fronty odpovědí
- Odpovědi na lokální fronty
- Definice kanálů zpráv

Další informace o konceptech, které se podílejí na používání těchto objektů, najdete v tématu “Konfigurace distribuovaných front” na stránce 171.

Kanály musí být zcela definovány a jejich přidružené objekty musí existovat a musí být k dispozici pro použití, než bude možné spustit kanál.

Kromě toho musí být pro každý kanál definován a dostupný konkrétní komunikační spoj, aby bylo možné kanál spustit. Popis toho, jak jsou definovány propojení LU 6.2 a TCP/IP, najdete v konkrétní komunikační příručce pro vaši instalaci.

Procedura

- Další informace o vytváření a práci s objekty naleznete v následujících tématech:

- “Vytváření objektů v systému IBM i” na stránce 245
- “Vytvoření kanálu v systému IBM i” na stránce 245
- “Spuštění kanálu v systému IBM i” na stránce 247
- “Výběr kanálu v systému IBM i” na stránce 248
- “Procházení kanálu v systému IBM i” na stránce 248
- “Přejmenování kanálu v systému IBM i” na stránce 250
- “Práce se stavem kanálu v systému IBM i” na stránce 250
- “Volby Work-with-channel na systému IBM i” na stránce 251

Související pojmy

“Nastavení komunikace pro IBM i” na stránce 257
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby mohla být úspěšná, je nezbytné, aby připojení bylo definováno a dostupné.

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 kanálů zpráv pro produkt IBM MQ for IBM i
Příkazy CL produktu IBM MQ for IBM i

IBM i Vytváření objektů v systému IBM i

K vytvoření fronty a objektů aliasů můžete použít příkaz CRTMQMQ.

Můžete vytvořit frontu a objekty aliasu, jako jsou přenosové fronty, definice vzdálených front, definice alias správce front, definice aliasů fronty odpovědí a odpovědi na lokální fronty.

Chcete-li zobrazit seznam výchozích objektů, prohlédněte si téma 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:

1. Použijte F6 z panelu Práce s kanály MQM (WRKMQMCHL).

   Případně použijte příkaz CRTMQMCHL z příkazového řádku.

   Ať tak či onak, zobrazí se panel Vytvoření kanálu. Typ:

   - Název kanálu v poskytnutém poli
   - Typ kanálu pro tento konec odkazu
2. Stiskněte klávesu Enter.

Poznámka: Všechny kanály ve vaší síti musíte pojmenovat jedinečným způsobem. Jak je zobrazeno v Síťový diagram zobrazující všechny kanály, včetně názvů zdrojového a cílového správce front v názvu kanálu je dobrý způsob, jak to provést.

Vaše položky se validují a chyby jsou nahlášeny okamžitě. Opravte všechny chyby a pokračujte.

Pro typ kanálu, který jste vybrali, se zobrazí příslušný panel nastavení kanálu. Vyplňte pole spolu s informacemi, které jste shromáždili dříve. Stisknutím klávesy Enter vytvořte kanál.

Poskytujete vám pomoc při rozhodování o obsahu různých polí v popisech panelů definice kanálu na panelech nápovědy a v části Atributy kanálu.

```
Create MQM Channel (CRTMQMCHL)

Type choices, press Enter.

Channel name . . . . . > CHANNAME_____________
Channel type . . . . . > *SDR__    *RCVR, *SDR, *SVR, *RQSTR...
Message Queue Manager name     *DFT_____________________________
_____
Replace . . . . . .  *NO_     *NO, *YES
Transport type . . . . . .  *TCP____   *LU62, *TCP, *SYSDFTCHL
Text 'description' . . . . . > 'Example Channel Definition'_____________
_____________________________
Connection name . . . . . .  *SYSDFTCHL_____________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________
More...
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 27. 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 28. 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 29. 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 30. 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 moduly listener SNA musíte nakonfigurovat komunikační subsystém.

Aby aplikace mohly vyměňovat zprávy, musíte spustit program listener pro příchozí připojení za použití příkazu STRMQMLSR.

V případě odchozích připojení je třeba kanál spustit jedním z následujících způsobů:

1. Použijte příkaz CL STRMQMCHL, který uvádí název kanálu, abyste spustili kanál jako proces nebo podproces, v závislosti na parametru MCATYPE. (Jsou-li kanály spouštěny jako podprocesy, jsou podprocesy iniciátoru kanálu.)

```
STRMQMCHL CHLNAME(QM1.TO.QM2) MQNAME(MYQMGR)
```

2. Použijte inicializátor kanálu ke spuštění kanálu. Inicializátor jednoho kanálu se spustí automaticky při spuštění správce front. Tento automatický start lze eliminovat změnou sekce chinit v souboru qm.ini pro daného správce front.
3. Použijte příkaz WRKMQMCHL pro zahájení práce s panelem Práce s kanály a vyberte volbu 14 pro spuštění kanálu.

IBM i Výběr kanálu v systému IBM i

Kanál můžete vybrat na panelu Práce s kanály.

Chcete-li vybrat kanál, použijte příkaz WRKMQMCHL, abyste mohli začít na panelu Práce s kanály:

1. Přesuňte kurzor na pole voleb přidružené k požadovanému názvu kanálu.
2. Zadejte číslo volby.
3. Stisknutím klávesy Enter aktivujete svou volbu.

Vyberete-li více než jeden kanál, volby se aktivují v posloupnosti.

```
Work with MQM Channels

Queue Manager Name . . :  CNX

Type options, press Enter.
2=Change  3=Copy  4=Delete  5=Display  8=Work with Status  13=Ping
14=Start  15=End  16=Reset  17=Resolve

Opt   Name           Type    Transport   Status
CHLNIC          *RCVR    *TCP     INACTIVE
CORSAIR.TO.MUSTANG    *SDR    *LU62    INACTIVE
FV.CHANNEL.MC.DJE1    *RCVR    *TCP     INACTIVE
FV.CHANNEL.MC.DJE2    *SDR    *TCP     INACTIVE
FV.CHANNEL.MC.DJE3    *RQSTR   *TCP     INACTIVE
FV.CHANNEL.MC.DJE4    *SVR    *TCP     INACTIVE
FV.CHANNEL.PETER     *RCVR    *TCP     INACTIVE
FV.CHANNEL.PETER.LU   *RCVR    *LU62    INACTIVE
FV.CHANNEL.PETER.LU1   *RCVR    *LU62    INACTIVE
More...
Parameters or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Create  F9=Retrieve  F12=Cancel
F21=Print
```

Obrázek 31. Práce s kanály

IBM i Procházení kanálu v systému IBM i

Kanál můžete procházet z panelu Zobrazení kanálu nebo pomocí příkazu DSPMQMCHL na příkazovém řádku.

Chcete-li procházet nastavení kanálu, použijte příkaz WRKMQMCHL a začněte na panelu Zobrazení kanálu:

1. Zadejte volbu 5 (Zobrazení) proti požadovanému názvu kanálu.
2. Stisknutím klávesy Enter aktivujete svou volbu.

Vyberete-li více než jeden kanál, budou uvedeny v posloupnosti.

Případně můžete použít příkaz DSPMQMCHL z příkazového řádku.

Výsledkem je zobrazení příslušného panelu Zobrazení kanálu s podrobnostmi o aktuálních nastaveních pro kanál. Pole jsou popsána v části Atributy kanálu.

```
Display MQM Channel

Channel name . . . . . :  ST.JST.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 32. Zobrazit kanál TCP/IP (1)

```
Display MQM Channel

Short retry interval . . . . . :  60
Short retry count . . . . . :  10
Long retry interval . . . . . :  6000
Long retry count . . . . . :  10
Security exit . . . . . :
Library . . . . . :
Security exit user data . . . :
Send exit . . . . . :
Library . . . . . :
Send exit user data . . . . . :
Receive exit . . . . . :
Library . . . . . :
Receive exit user data . . . . :
Message exit . . . . . :
Library . . . . . :
Message exit user data . . . . :
More...



F3=Exit  F12=Cancel  F21=Print
```

Obrázek 33. Zobrazit kanál TCP/IP (2)

```
Display MQM Channel

Sequence number wrap . . . . . :  999999999
Maximum message length . . . . :  10000
Convert message . . . . . :  *NO
Heartbeat interval . . . . . .  300
Nonpersistent message speed . .  *FAST









Bottom



F3=Exit  F12=Cancel  F21=Print
```

Obrázek 34. Zobrazit kanál 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. Použijte volbu 3 (Kopírování) pro vytvoření duplikátu s novým názvem.
3. Použijte volbu 5 (Zobrazení), abyste zkontrolli, že byla vytvořena správně.
4. Použijte volbu 4 (Delete) k odstranění původního kanálu.

Pokud se rozhodnete přejmenovat kanál zpráv, ujistěte se, že oba konce kanálu jsou přejmenovány ve stejnou dobu.

IBM i Práce se stavem kanálu v systému IBM i

S stavem kanálu můžete pracovat na panelu Práce se stavem kanálu.

Použijte příkaz WRKMQMCHST k zobrazení první sady panelů, které zobrazují stav vašich kanálů. Panely stavu v posloupnosti můžete zobrazit, když vyberete volbu Změnit zobrazení (F11).

Případně, výběrem volby 8 (Práce se stavem) z panelu Práce s kanály MQM se také zobrazí první stavový panel.

```
MQSeries Work with Channel Status

Type options, press Enter.
5=Display  13=Ping  14=Start  15=End  16=Reset  17=Resolve


Opt Name          Connection      Indoubt   Last Seq
CARTS_CORSAIR_CHAN  GBIBMIYA.WINSDOA1    NO        1
CHLNIC        9.20.2.213       NO        3
FV.CHANNEL.PETER2   9.20.2.213       NO      6225
JST.1.2        9.20.2.201       NO       28
MP_MUST_TO_CORS    9.20.2.213       NO       100
MUSTANG.TO.CORSAIR  GBIBMIYA.WINSDOA1    NO       10
MP_CORS_TO_MUST    9.20.2.213       NO       101
JST.2.3        9.5.7.126        NO       32
PF_WINSDOA1_LU62   GBIBMIYA.IYA80020    NO       54
PF_WINSDOA1_LU62   GBIBMIYA.WINSDOA1    NO       500
ST.JCW.EXIT.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 35. První ze sady stavových panelů kanálu

Volby, které jsou k dispozici na panelu Práce se stavem kanálu, jsou:

Volba nabídky	Popis
5=Display	Zobrazí nastavení kanálu.
13=Ping	Inicializuje akci Ping, kde je to vhodné.
14=Start	Spustí kanál.
15=End	Zastaví kanál.
16=Reset	Vynuluje pořadové číslo kanálu.
17=Resolve	Řeší situaci v nejistém stavu, ručně.

IBM i Volby 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 proti vybraným kanálům.

Volby, které jsou k dispozici na panelu Práce s kanály, jsou:

Volba nabídky	Popis
“2=Change” na stránce 252	Změní atributy kanálu.
“3=Copy” na stránce 252	Zkopíruje atributy kanálu do nového kanálu.
“4=Delete” na stránce 252	Odstraní kanál.
“5=Display” na stránce 252	Zobrazí aktuální nastavení pro kanál.
“6=Create” na stránce 253	Zobrazí panel Vytvořit kanál
“8=Work se stavem” na stránce 253	Zobrazí stavové panely kanálu.

Volba nabídky	Popis
“13=Ping” na stránce 254	Spustí poskytovanou službu PING tak, aby otestuje spojení se sousedním systémem pomocí výměny pevné datové zprávy se vzdáleným koncem.
“14=Start” na stránce 254	Spustí vybraný kanál nebo resetuje zablokovaný přijímací kanál.
“15=End” na stránce 255	Požaduje uzavření kanálu.
“16=Reset” na stránce 256	Požaduje, aby kanál resetoval pořadová čísla na tomto konci spojení. Čísla musí být stejná na obou koncích, aby se kanál mohl spustit.
“17=Resolve” na stránce 256	Požaduje, aby kanál interpretoval neověřené zprávy bez navázání spojení s druhým koncem.
“18=Zobrazení oprávnění” na stránce 256	Zobrazí oprávnění k objektu IBM MQ
“19=Udělení oprávnění” na stránce 256	Uděluje oprávnění k objektu IBM MQ
“20=Odvolání oprávnění” na stránce 256	Odvolá oprávnění k objektu IBM MQ
“21=Zotavit objekt” na stránce 257	Obnovený objekt IBM MQ
“22=Záznam obrazu” na stránce 257	Obraz objektu IBM MQ záznamů

IBM i 2=Change

Chcete-li změnit existující definici kanálu, použijte volbu Změna.

Volba Změna, nebo příkaz CHGMQMCHL mění existující definici kanálu, kromě názvu kanálu. Přepište pole, která se mají změnit na panelu definice kanálu, a poté uložte aktualizovanou definici stisknutím klávesy Enter.

IBM i 3=Copy

Použijte volbu Kopírovat ke kopírování existujícího kanálu.

Volba Kopírování používá příkaz CPYMQMCHL ke kopírování existujícího kanálu. Panel Kopírování vám umožňuje definovat nový název kanálu. Tyto znaky však musíte omezit na znaky, které jsou platné pro názvy objektů produktu IBM i , viz téma Administrace produktu IBM MQ for IBM i.

Stisknutím klávesy Enter na panelu Kopírování zobrazíte podrobnosti o aktuálních nastaveních. Můžete změnit libovolné nové nastavení kanálu. Novou definici kanálu uložte stisknutím klávesy Enter.

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

Pomocí volby Zobrazit můžete zobrazit aktuální definice pro kanál.

Tato volba zobrazí panel s poli zobrazenými aktuálními hodnotami parametrů a chráněný proti vstupu uživatele.

IBM i 6=Create

Pomocí volby Create můžete zobrazit panel Vytvořit kanál.

Použijte volbu Create, nebo zadejte příkaz CRTMQMCHL z příkazového řádku, abyste získali panel Vytvořit kanál. K dispozici jsou příklady panelů Vytvořit kanál, které začínají v Obrázek 27 na stránce 246.

Prostřednictvím tohoto panelu můžete vytvořit definici kanálu z obrazovky polí vyplněných výchozími hodnotami dodanými produktem IBM MQ for IBM i. Zadejte název kanálu, vyberte typ kanálu, který vytváříte, a metodu komunikace, která má být použita.

Stisknete-li Enter, zobrazí se panel. Zadejte informace do všech požadovaných polí na tomto panelu a zbývající panely a poté uložte definici stisknutím klávesy Enter.

Název kanálu musí být stejný na obou koncích kanálu a musí být jedinečný v rámci sítě. Musíte však omezit znaky použité na tyto znaky, které jsou platné pro názvy objektů produktu IBM MQ for IBM i .

Pro některá pole mají všechny panely výchozí hodnoty zadané v produktu IBM MQ for IBM i . Tyto hodnoty můžete upravit, nebo je můžete změnit, když vytváříte nebo kopírujete kanály. Chcete-li upravit hodnoty, podívejte se na *IBM MQ for IBM i System Administration*.

Můžete vytvořit vlastní sadu výchozích hodnot kanálu tak, že nastavíte fiktivní kanály s požadovanými výchozími hodnotami pro každý typ kanálu a zkopírujete je pokaždé, když chcete vytvořit nové definice kanálu.

Související odkazy

Atributy kanálu

IBM i 8=Work se stavem

Chcete-li zobrazit podrobné informace o stavu kanálu, použijte volbu Práce se stavem.

Sloupec Stav informuje o tom, zda je kanál aktivní nebo neaktivní, a že je průběžně zobrazen na panelu Práce s kanály MQM. Použijte volbu 8 (Práce se stavem), abyste viděli více zobrazených informací o stavu. Alternativně lze tyto informace zobrazit z příkazového řádku pomocí příkazu WRKMQMCHST. Viz “Práce se stavem kanálu v systému IBM i” na stránce 250.

- Název kanálu
- Typ kanálu
- Stav kanálu
- Instance kanálu
- Vzdálený správce front
- Jméno přenosové fronty
- Název komunikačního připojení
- Stav nejistého stavu kanálu
- Poslední pořadové číslo
- Počet nejistých zpráv
- Pořadové číslo, které vyvolává pochybnosti
- Počet zpráv v přenosové frontě
- Identifikátor logické pracovní jednotky
- Identifikátor logické pracovní jednotky v nejistém stavu
- Dílčí stav kanálu
- Monitorování kanálů
- Komprese záhlaví
- Komprese zpráv
- Indikátor doby komprese
- Ukazatel míry komprese

- Indikátor doby přenosové fronty
- Indikátor doby sítě
- Indikátor času ukončení
- Indikátor velikosti dávky
- Aktuální sdílené konverzace
- Maximum sdílených konverzací

IBM i *13=Ping*

Použijte volbu PING k výměně pevné datové zprávy se vzdáleným koncem.

A successful IBM MQ Ping gives some confidence to the system supervisor that the channel is available and functioning.

Příkaz ping nezahrnuje použití přenosových front a cílových front. Používá definice kanálu, související komunikační linku a nastavení sítě.

Je k dispozici pouze pro kanály odesílatele a serveru. Odpovídající kanál se spustí na vzdálené straně odkazu a provede dohodnutí spouštěcího parametru. Chyby jsou oznámeny normálně.

Výsledek výměny zpráv se zobrazí na panelu PING pro vás a je vráceným textem zprávy spolu s časem odeslání zprávy a časem přijetí odpovědi.

Příkaz ping s LU 6.2

Je-li příkaz PING vyvolán v produktu IBM MQ for IBM i, spouští se s ID uživatele požadujícího funkci, zatímco normální způsob, jakým je spuštěn program kanálu, je určen pro ID uživatele QMQM, které má být převzato pro kanály kanálu. ID uživatele proudí do přijímající strany a musí být platné na přijímajícím konci konverzace LU 6.2 , která má být alokována.

IBM i *14=Start*

Chcete-li spustit kanál ručně, použijte volbu Spustit.

Volba Start je k dispozici pro kanály odesílatele, serveru a žadatele. Není nutné, aby byl kanál nastaven se spuštěním správce front.

Volba Start se také používá pro kanály příjemce, připojení k serveru, odesilatele klastru a příjemce klastru. Spouštění přijímacího kanálu, který je ve stavu STOPPED, znamená, že jej lze spustit ze vzdáleného kanálu.

Když je spuštěna, odesílající agent MCA přečte definiční soubor kanálu a otevře přenosovou frontu. Je vydána spouštěcí posloupnost kanálu, která vzdáleně spustí odpovídající MCA přijímače nebo kanálu serveru. Po spuštění budou procesy odesílatele a serveru čekat na zprávy přicházející do přenosové fronty a předávají je, jakmile dorazí.

Když používáte spouštěcí impuls, musíte spustit stále běžící spouštěcí proces, abyste monitorovali inicializační frontu. Příkaz STRMQMCHLI lze použít pro spuštění procesu.

Na vzdáleném konci kanálu může být přijímající proces spuštěn jako odezva na spuštění kanálu z odesílajícího konce. Tato metoda se liší pro LU 6.2 a TCP/IP připojené kanály:

- LU 6.2 připojených kanálů nevyžaduje žádnou explicitní akci na přijímajícím konci kanálu.
- Připojené kanály protokolu TCP vyžadují, aby byl proces modulu listener spuštěn nepřetržitě. Tento proces čeká na požadavky na spuštění kanálu od vzdáleného konce odkazu a spustí proces definovaný v definicích kanálu pro dané připojení.

  Je-li vzdálený systém IBM i, můžete použít příkaz STRMQMLSR.

Použití volby Start vždy způsobí, že se kanál resynchronizuje, je-li to nutné.

Aby bylo možné začít úspěšně:

- Definice kanálů, lokální a vzdálené musí existovat. Pokud neexistuje vhodná definice kanálu pro přijímací kanál nebo kanál připojení serveru, vytvoří se automaticky, je-li kanál automaticky definován, automaticky. Viz Channel auto-definition exit program.
- Přenosová fronta musí existovat, musí být povolena pro GET a nemají žádné jiné kanály používající ji.
- MCAs, místní a vzdálený, musí existovat.
- Komunikační spojení musí být dostupné.
- Správci front musí být spuštění, lokálními a vzdálenými.
- Kanál zpráv musí být neaktivní.

Chcete-li přenášet zprávy, vzdálené fronty a definice vzdálených front musí existovat.

Zobrazí se panel potvrzující, že požadavek na spuštění kanálu byl přijat. Chcete-li potvrdit, že úvodní proces byl úspěšný, zkontrolujte systémový protokol nebo stiskněte klávesu F5 (obnovte obrazovku).

IBM i *15=End*

Aktivita kanálu slouží k zastavení aktivity kanálu.

Pomocí volby Ukončit lze požádat kanál o zastavení aktivity. Kanál neodešle žádné další zprávy.

Před stisknutím klávesy Enter vyberte volbu F4 a zvolte, zda se kanál stane ZASTAVENO nebo NEAKTIVNÍ, a zda má být kanál zastaven pomocí ŘADIČE nebo zastavení IMMEDIATE. Zastavený kanál musí být znovu spuštěn operátorem, aby se znovu aktivoval. Může být spuštěn neaktivní kanál.

Okamžité zastavení

Použijte okamžité zastavení k zastavení kanálu bez dokončení libovolné jednotky práce.

Tato volba ukončuje proces kanálu. Výsledkem je, že kanál nedokončí zpracování aktuální dávky zpráv, a proto nemůže kanál v nejistém stavu opustit kanál. Obecně platí, že je lepší, aby operátoři mohli používat volbu řízeného zastavení.

Zastavit řízené

Pomocí příkazu Stop lze zastavit kanál na konci aktuální jednotky práce.

Tato volba požaduje, aby kanál byl ukončen řádným způsobem; aktuální dávka zpráv je dokončena a procedura synchronizačního bodu se provádí s druhým koncem kanálu.

Restartování zastavených kanálů

Když kanál přejde do stavu ZASTAVENO, je třeba kanál restartovat ručně. Kanál můžete restartovat následujícími způsoby:

- Pomocí příkazu **START CHANNEL** MQSC.
- Pomocí příkazu **Start Channel** PCF.
- Pomocí produktu IBM MQ Explorer.
- z/OS V systému z/OSpomocí panelu Spustit kanál.
- IBM i V systému IBM ipomocí příkazu **STRMQMCHL CL** nebo volby **ZAČÁTEK** na panelu WRKMQMCHL.

V případě odesílatelů nebo kanálů serveru, kdy kanál vstoupil do stavu STOPPED, byla přidružená přenosová fronta nastavena na GET (DISABLED) a spuštění bylo vypnuto. Když je přijat požadavek na spuštění, tyto atributy se resetují automaticky.

z/OS Pokud se inicializátor kanálu zastaví, zatímco se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu inicializátoru kanálu. Stav kanálu pro typ kanálu SVRCONN se však resetuje, pokud se zastaví inicializátor kanálu v době, kdy je kanál ve stavu ZASTAVENO.

Multi Pokud se správce front zastaví v případě, že se kanál nachází ve stavu RETRYING nebo STOPPED, je stav kanálu zapamatován při restartu správce front. Od verze IBM MQ 8.0 se tato vztahuje také na kanály SVRCONN. Dříve byl stav kanálu pro typ kanálu SVRCONN resetován, pokud byl inicializátor kanálu zastaven v době, kdy byl kanál ve stavu ZASTAVENO.

IBM i *16=Reset*

Chcete-li vynutit novou posloupnost zpráv, použijte volbu Reset.

Volba Reset změní pořadové číslo zprávy. Používejte jej opatrně a pouze poté, co jste použili volbu Vyřešit k vyřešení všech situací, které jsou v nejistém stavu. Tato volba je k dispozici pouze u odesílacího kanálu nebo kanálu serveru. První zpráva začíná novou posloupností při příštím spuštění kanálu.

IBM i *17=Resolve*

Použijte volbu Vyřešit, abyste vynutili lokální potvrzení nebo vrácení neověřených zpráv, které se nacházejí v přenosové frontě.

Použijte volbu Vyřešit, když zprávy jsou drženy v nejistém stavu odesilatelem nebo serverem, například protože jeden konec odkazu byl ukončen a není zde žádná vyhlídka na obnovení. Volba Vyřešit přijímá jeden ze dvou parametrů: BACKOUT nebo COMMIT. Funkce Backout obnovuje zprávy do přenosové fronty, zatímco operace Commit je vyřazuje.

Program kanálu se nepokusí o vytvoření relace s partnerem. Místo toho určí identifikátor logické jednotky práce (LUWID), který reprezentuje neověřené zprávy. Podle požadavku se pak vydává buď:

- BACKOUT pro obnovení zpráv do přenosové fronty; nebo
- COMMIT pro odstranění zpráv z přenosové fronty.

Aby bylo řešení úspěšné, postupujte takto:

- Kanál musí být neaktivní
- Kanál musí mít pochybnosti.
- Typ kanálu musí být odesilatel nebo server
- Definice kanálu, lokální, musí existovat
- Správce front musí být spuštěn, lokální

IBM i *18=Zobrazení oprávnění*

Volbu Zobrazení oprávnění použijte k zobrazení toho, jaké akce má uživatel oprávnění provádět na specifickém objektu IBM MQ .

Pro vybraný objekt a uživatele zobrazí příkaz DSPMQAUT oprávnění, která má uživatel k provádění akcí na objektu IBM MQ . Je-li uživatel členem více skupin, pak příkaz zobrazí kombinovanou autorizaci všech skupin k objektu.

IBM i *19=Udělení oprávnění*

Použijte volbu Udělit oprávnění, abyste udělili oprávnění provádět akce s objekty IBM MQ jinému uživateli nebo skupině uživatelů.

Příkaz GRTMQMAUT je k dispozici pouze pro uživatele ve skupině QMQMADM. Uživatel v QMQMADM uděluje oprávnění jiným uživatelům provádět akce na objektech IBM MQ uvedených v příkazu buď identifikací uživatelů podle jména, nebo udělením oprávnění všem uživatelům v *PUBLIC.

IBM i *20=Odvolání oprávnění*

Oprávnění k odebrání oprávnění k provádění akcí na objektech od uživatelů lze odebrat pomocí oprávnění Odebrat oprávnění.

Příkaz RVKMQMAUT je k dispozici pouze pro uživatele ve skupině QMQMADM. Uživatel ve skupině QMQMADM odstraní oprávnění od jiných uživatelů k provádění akcí na objektech IBM MQ vyjmenovaných

v příkazu buď identifikováním uživatelů podle jména, nebo zrušením oprávnění od všech uživatelů v *PUBLIC.

IBM i 21=Zotavit objekt

Použijte Obnova objektu k obnově poškozených objektů z informací uložených v žurnálech IBM MQ .

Obnova objektu používá příkaz RCRMQMOBJ (Re-create MQ Object) k obnově všech objektů, které jsou v příkazu poškozeny. Pokud objekt není poškozen, neprovede se žádná akce na daném objektu.

IBM i 22=Záznam obrazu

Použijte obraz záznamu ke snížení počtu žurnálových zásobníků požadovaných pro obnovu sady objektů a k minimalizaci doby obnovy.

Příkaz RCDMQMIMG má kontrolní bod pro všechny objekty, které jsou vybrány v příkazu. Synchronizuje aktuální hodnoty objektů v integrovaném systému souborů (IFS) s pozdějšími informacemi o objektech, jako jsou operace MQPUTs a MQGET zaznamenané v žurnálových zásobnících.

Když příkaz dokončí objekty v IFS, jsou aktuální a tyto žurnálové zásobníky již nemusí být přítomny, aby mohly být objekty napravovány. Všechny odpojené žurnálové zásobníky mohou být odpojeny (pokud není požadováno, aby mohly být 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. Aby mohla být úspěšná, je nezbytné, aby připojení bylo definováno a dostupné.

DQM je prostředek vzdáleného řazení do fronty pro produkt IBM MQ for IBM i. Poskytuje řídicí programy kanálu pro správce front produktu IBM MQ for IBM i , které tvoří rozhraní pro komunikační spojení, které lze řídit operátorem systému.

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Aby mohla být úspěšná, je nezbytné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak zajistit, aby připojení bylo definováno a dostupné.

Před spuštěním kanálu musí být přenosová fronta definována způsobem popsaným v této části a musí být zahrnuta do definice kanálu zpráv.

Mezi systémy IBM MQ for IBM i můžete vybrat ether následujících dvou způsobů komunikace:

- “Definování připojení TCP na systému IBM i” na stránce 258

  Pro protokol TCP lze použít adresu hostitele a tato připojení jsou nastavena tak, jak je popsáno v příručce *IBM i Communication Configuration Reference*.

  V prostředí TCP je každá distribuovaná služba alokována jedinečnou adresou TCP, kterou mohou používat vzdálené počítače pro přístup ke službě. Adresa TCP se skládá z názvu hostitele/čísla a čísla portu. Všichni správci front používají takové číslo ke vzájemné komunikaci prostřednictvím protokolu TCP.
- “Příjem na TCP” na stránce 258

  Tato forma komunikace vyžaduje definici logické jednotky IBM i SNA typu 6.2 (LU 6.2), která poskytuje fyzický spoj mezi systémem IBM i obsluhujícím lokálního správce front a systémem obsluhujícím vzdáleného správce front. Podrobnosti o konfiguraci komunikací v produktu IBM inajdete v příručce *IBM i Communication Configuration Reference* .

V případě potřeby musí být spouštěcí mechanismus připraven také s definicí nezbytných procesů a front.

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Související úlohy

"Monitorování a řízení kanálů v systému IBM i" na stránce 244
Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front. Každý správce front má program DQM pro řízení propojení mezi kompatibilními vzdálenými správci front.

Související odkazy

Příklad konfigurace- IBM MQ for IBM i
Příklad plánování kanálů zpráv pro produkt IBM MQ for IBM i
Interkomunikační úlohy v systému IBM i
Stav kanálů v systému IBM i

IBM i *Definování připojení TCP na systému IBM i*

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

Definice kanálu obsahuje pole CONNECTION NAME, které obsahuje buď síťovou adresu TCP cíle, nebo název hostitele (například ABCHOST). Síťová adresa TCP může být v tečkovém desítkovém tvaru IPv4 (například 127.0.0.1) nebo v hexadecimální formě IPv6 (například 2001:DB8:0:0:0:0:0:0). Pokud je NÁZEV PŘIPOJENÍ název hostitele nebo server názvů, tabulka hostitelů IBM i se používá k převedení názvu hostitele na adresu hostitele TCP.

Číslo portu je povinné pro úplnou adresu TCP; pokud toto číslo není dodáno, použije se výchozí číslo portu 1414. Na zahajovacím konci připojení (typy kanálů odesílatele, žadatele a serveru) je možné poskytnout volitelné číslo portu pro připojení, například:

```
Connection name 127.0.0.1 (1555)
```

V tomto případě se iniciující ukončení pokusí připojit k přijímajícímu programu na portu 1555.

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Použití volby nevyřízených požadavků na modul listener TCP

V protokolu TCP se zachází s neúplnými připojeními, pokud se mezi serverem a klientem nekoná trojstranná komunikace výměnou potvrzení. Tato připojení se nazývají nevyřízené požadavky na připojení. Pro tyto nevyřízené požadavky na připojení je nastavena maximální hodnota a lze ji považovat za nahromadění požadavků čekajících na portu TCP, aby modul listener přijal požadavek.

Viz "Použití volby seznamu požadavků na modul listener TCP v systému IBM MQ for Multiplatforms" na stránce 241 , kde získáte další informace, a specifickou hodnotu pro IBM i.

Související pojmy

"Příjem na TCP" na stránce 258
Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu. Chcete-li odpovědět na požadavek na spuštění, je třeba spustit program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu STRMQMLSR.

IBM i *Příjem na TCP*

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu. Chcete-li odpovědět na požadavek na spuštění, je třeba spustit program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu STRMQMLSR.

Pro každého správce front můžete spustit více než jeden modul listener. Ve výchozím nastavení příkaz STRMQMLSR používá port 1414, ale tuto hodnotu můžete přepsat. Chcete-li přepsat výchozí nastavení, přidejte následující příkazy do souboru qm.ini vybraného správce front. V tomto příkladu je listener požadován pro použití portu 2500:

```
TCP:
Port=2500
```

Soubor qm.ini se nachází v tomto adresáři IFS: /QIBM/UserData/mqm/qmgrs/ *název správce front*.

Tato nová hodnota se načte pouze v případě, že je spuštěn modul listener TCP. Máte-li již spuštěný modul listener, nebude tento program tento program vidět. Chcete-li použít novou hodnotu, zastavte modul listener a znovu zadejte příkaz STRMQMLSR. Nyní, kdykoli použijete příkaz STRMQMLSR, je listener standardně nastaven na nový port.

Případně můžete zadat jiné číslo portu v příkazu STRMQMLSR. Příklad:

```
STRMQMLSR MQMNAME( queue manager name ) PORT(2500)
```

Tato změna způsobí, že modul listener bude standardně nastaven na nový port po dobu trvání úlohy modulu listener.

Použití volby TCP SO_KEEPALIVE

Chcete-li použít volbu SO_KEEPALIVE (další informace viz “Kontrola, zda je druhý konec kanálu stále k dispozici” na stránce 206) Do konfiguračního souboru správce front (qm.ini v adresáři IFS, /QIBM/UserData/mqm/qmgrs/ *název správce front*) je třeba přidat následující položku:

```
TCP:
KeepAlive=yes
```

Pak musíte zadat následující příkaz:

```
CFGTCP
```

Vyberte volbu 3 (Change TCP Attributes). Nyní můžete zadat časový interval v minutách. Můžete zadat hodnotu v rozsahu 1 až 40320 minut; výchozí hodnota je 120.

Použití volby nevyřízených požadavků na modul listener TCP

Při příjmu na protokolu TCP je nastaven maximální počet neprovedených požadavků na připojení. Toto číslo může být považováno za *nevyřízené požadavky* požadavků čekajících na port TCP pro modul listener, aby přijal požadavek.

Výchozí hodnota nahromadění modulu listener v systému IBM i je 255. Pokud velikost nevyřízených požadavků dosáhne této hodnoty, připojení TCP se odmítne a kanál nebude možné spustit.

V případě kanálu MCA se výsledkem tohoto výsledku v kanálu stane stav ZOPAKOVAT a později se znovu pokusí o připojení.

V případě připojení klienta obdrží klient kód příčiny MQRC_Q_MGR_NOT_AVAILABLE z objektu MQCONN a později se může připojení pokusit o zopakování připojení.

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

```
ListenerBacklog = n
```

Tento parametr přepíše výchozí maximální počet nevyřízených požadavků (255) pro modul listener TCP.

Poznámka: Některé operační systémy podporují větší hodnotu, než je výchozí. V případě potřeby lze tuto hodnotu použít, abyste se vyhnuli dosažení limitu připojení.

IBM i *Definování připojení LU 6.2 na systému IBM i*

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

Iniciovaný konec odkazu musí mít definici směrovacího záznamu, aby doplňoval tento objekt CSI. Další informace o správě pracovních požadavků ze vzdálených logických jednotek LU 6.2 jsou k dispozici v příručce *IBM i Programming: Work Management Guide*.

Informace naleznete v příručce *Multiplatform APPC Configuration Guide* a v následující tabulce.

Tabulka 26. Nastavení na lokálním systému IBM i pro vzdálenou platformu správce front

Vzdálená platforma	**TPNAME**
z/OS nebo MVS	Totéž jako v příslušných vedlejších informacích o vzdáleném správci front.
IBM i	Stejné jako porovnávací hodnota v záznamu směrování v systému IBM i .
Systémy UNIX and Linux	Invovatelný transakční program definovaný ve vzdálené konfiguraci LU 6.2 .
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nezvolnitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.

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

Související pojmy

“Zahájení ukončení (Odesilatel)” na stránce 260
Použijte příkaz CRTMQMCHL, abyste definovali kanál typu přenosu *LU62.

“Iniciovaný konec (přijímač)” na stránce 263
Použijte příkaz CRTMQMCHL, abyste definovali přijímací konec propojení kanálu zpráv s typem přenosu *LU62.

IBM i *Zahájení ukončení (Odesilatel)*

Použijte příkaz CRTMQMCHL, abyste definovali kanál typu přenosu *LU62.

Použití objektu CSI je volitelné v produktu IBM MQ for IBM i V5.3 nebo pozdější.

Zahajovací panel se zobrazí na obrázku LU 6.2 -úvodní panel pro nastavení komunikace. Chcete-li získat úplný panel podle obrázku, stiskněte klávesu F10 z prvního panelu.

```
Create Comm Side Information (CRTCSI)

Type choices, press Enter.

Side information . . . . . > WINSDOA1   Name
Library . . . . . >  QSYS    Name, *CURLIB
Remote location . . . . . > WINSDOA1   Name
Transaction program . . . . . > MQSERIES

Text 'description' . . . . . .  *BLANK


Additional Parameters

Device . . . . . .  *LOC     Name, *LOC
Local location . . . . . .  *LOC     Name, *LOC, *NETATR
Mode . . . . . .  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 36. Panel inicializace komunikace LU 6.2 -počáteční ukončení

Vyplňte pole iniciace, jak je uvedeno:

Informace o připojení
Zadejte název, který se použije k uložení objektu informací o připojení, který má být vytvořen, například WINSDOA1.

Poznámka: Pro LU 6.2je to propojení mezi definicí kanálu zpráv a komunikačním připojením pole **Název připojení** definice kanálu zpráv na odesílajícím konci. Toto pole obsahuje název objektu CSI.

Knihovna
Název knihovny, kde je uložena tato definice.

Objekt CSI musí být dostupný v knihovně přístupné pro program obsluhující kanál zpráv, například QSYS, QMQM a QGPL.

Je-li název nesprávný, chybí nebo jej nelze najít, dojde k chybě při spuštění kanálu.

Vzdálené umístění
Uvádí jméno vzdáleného systému, se kterým váš program komunikuje.

Stručně řečeno, tento povinný parametr obsahuje název logické jednotky partnera na vzdáleném systému, jak je definováno v popisu zařízení, které se používá pro komunikační spojení mezi dvěma systémy.

Název **Vzdálený systém** lze nalézt zadáním příkazu DSPNETA na vzdálený systém a zobrazení předvoleného jména lokálního umístění.

Transakční program
Uvádí název (až 64 znaků) transakčního programu na vzdáleném systému, který se má spustit. Může se jednat o název procesu transakce, název programu, název kanálu nebo znakový řetězec, který odpovídá hodnotě **Porovnávací hodnota** v záznamu směrování.

Tento parametr je požadovaný.

Poznámka: Chcete-li zadat názvy transakčních programů služby SNA, zadejte hexadecimální znázornění názvu transakčního programu služby. Chcete-li například zadat název transakčního programu služby s hexadecimální reprezentací 21F0F0F1, zadali byste X'21F0F0F1'.

Další informace o jménech transakčních programů služby SNA najdete v publikaci *SNA Transaction Programmer's Reference* pro LU typu 6.2.

Je-li přijímající konec jiný systém IBM i , použije se název **transakčního programu** k porovnání objektu CSI na odesílajícím konci s položkou směrování na přijímajícím konci. Tento název musí být jedinečný

pro každého správce front v cílovém systému IBM i . Viz parametr **Program k volání** pod Initiated end (Receiver). Viz také parametr **comparison data: compare value** na panelu Přidání záznamu směrování.

Textový popis
Popis (až 50 znaků), který vám připomene zamýšlené použití tohoto připojení.

Zařízení
Uvádí jméno popisu zařízení použitého pro vzdálený systém. Možné hodnoty jsou:

*** UMÍSTĚNÍ**
Zařízení je určeno systémem.

jméno-zařízení
Uveďte jméno zařízení, které je přidruženo ke vzdálenému systému.

Lokální umístění
Uvádí název lokálního umístění. Možné hodnoty jsou:

*** UMÍSTĚNÍ**
Název lokálního umístění je určen systémem.

*** NETATR**
Použije se hodnota LCLLOCNAME uvedená v systémových atributech sítě.

Lokální-název-umístění
Uveďte název vašeho umístění. Uveďte lokální umístění, pokud chcete indikovat určité jméno umístění vzdáleného systému. Název umístění lze nalézt pomocí příkazu DSPNETA.

Režim
Uvádí režim používaný pro řízení relace. Tento název je stejný jako u rozhraní CPI (Common Programming Interface)-Communications Mode_Name. Možné hodnoty jsou:

*** NETATR**
Použije se režim v atributech sítě.

BLANK
Používá se osm prázdných znaků.

Název režimu
Uveďte jméno režimu pro vzdálené umístění.

Poznámka: Vzhledem k tomu, že režim určuje prioritu přenosu komunikační relace, může být užitečné definovat různé režimy v závislosti na prioritě odesílaných zpráv; například MQMODE_HI, MQMODE_MED a MQMODE_LOW. (Můžete mít více než jedno CSI odkazující na stejné umístění.)

Identifikátor vzdálené sítě
Uvádí identifikátor vzdálené sítě použitý se vzdáleným umístěním. Možné hodnoty jsou:

*** UMÍSTĚNÍ**
Použije se ID vzdálené sítě pro vzdálené umístění.

*** NETATR**
Použije se identifikátor vzdálené sítě uvedený v atributech sítě.

*** ŽÁDNÉ**
Vzdálená síť nemá žádný název.

ID-vzdálené-sítě
Uveďte ID vzdálené sítě. Pro vyhledání jména tohoto ID sítě použijte příkaz DSPNETA na vzdáleném umístění. Jedná se o 'ID lokální sítě' ve vzdáleném umístění.

Oprávnění
Uvádí oprávnění, které poskytujete uživatelům, kteří nemají určité oprávnění k objektu, kteří nejsou na seznamu oprávnění, a se skupinovým profilem, který nemá žádné specifické oprávnění k objektu. Možné hodnoty jsou:

*** LIBCRTAUT**
Veřejné oprávnění k objektu je převzato z parametru CRTAUT uvedené knihovny. Tato hodnota se určuje při vytvoření. Změní-li se hodnota parametru CRTAUT pro knihovnu po vytvoření objektu, nová hodnota neovlivní existující objekty.

*** ZMĚNA**
Oprávnění ke změně povoluje uživateli provádět základní funkce na objektu, avšak uživatel nemůže objekt změnit. Oprávnění ke změně poskytuje provozní oprávnění k objektu a oprávnění ke všem datům.

***ALL**
Uživatel může provádět všechny operace kromě těch operací, které jsou omezeny na vlastníka nebo jsou řízeny oprávněním ke správě seznamu oprávnění. Uživatel může řídit existenci objektu a určit zabezpečení objektu, změnit objekt a provádět základní funkce s objektem. Uživatel může měnit vlastnictví objektu.

*** POUŽITÍ**
Oprávnění k použití poskytuje provozní oprávnění k objektu a oprávnění ke čtení.

*** VYLOUČENÍ**
Vyloučit oprávnění zabraňuje uživateli v přístupu k objektu.

Seznam oprávnění
Uveďte jméno seznamu oprávnění s oprávněním, které se používá pro informace o připojení.

IBM i *Iniciovaný konec (přijímač)*

Použijte příkaz CRTMQMCHL, abyste definovali přijímací konec propojení kanálu zpráv s typem přenosu *LU62.

Ponechte pole Název PŘIPOJENÍ prázdné a ujistěte se, že odpovídající podrobnosti se shodují s odesláním konce kanálu. Podrobnosti naleznete v tématu Vytvoření kanálu.

Chcete-li povolit iniciaci ukončení přijímacího kanálu, přidejte do subsystému na zahájeném konci záznam směrování. Subsystém musí být ten, který alokuje zařízení APPC použité v relacích LU 6.2 . Proto musí mít pro toto zařízení platnou komunikační položku. Směrovací položka volá program, který spouští přijímající konec kanálu zpráv.

Použijte příkazy IBM i (například ADDRTGE) k definování konce odkazu, který je zahájen komunikační relací.

Zahájen koncový panel se zobrazí na panelu nastavení komunikace LU 6.2 -přidání záznamu směrování.

```
Add Routing Entry (ADDRTGE)

Type choices, press Enter.

Subsystem description . . . . .  QCMN     Name
Library . . . . . .   *LIBL    Name, *LIBL, *CURLIB
Routing entry sequence number .  1       1-9999
Comparison data:
Compare value . . . . . .  MQSERIES

Starting position . . . . . .  37      1-80
Program to call . . . . . .  AMQCRC6B   Name, *RTGDTA
Library . . . . . .  QMAS400    Name, *LIBL, *CURLIB
Class . . . . . .  *SBSD     Name, *SBSD
Library . . . . . .  *LIBL     Name, *LIBL, *CURLIB
Maximum active routing steps . .  *NOMAX    0-1000, *NOMAX
Storage pool identifier . . . .  1       1-10



Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Obrázek 37. Konec komunikačního zařízení LU 6.2 -zahájený konec

Popis podsystému
Název subsystému, ve kterém je umístěna tato definice. Použijte příkaz IBM i WRKSBSD k zobrazení a aktualizaci odpovídajícího popisu podsystému pro směrovací záznam.

Pořadové číslo položky směrování
Jedinečné číslo ve vašem subsystému pro identifikaci této definice komunikace. Můžete použít hodnoty v rozsahu 1-9999.

Porovnávací data: Porovnávací hodnota
Textový řetězec, který se má porovnat s řetězcem přijatým při spuštění relace parametrem **Transaction program** , jak ukazuje Obrázek 1. Znakový řetězec je odvozen z pole Transaction program odesílatele CSI.

Porovnávací údaje: počáteční pozice
Pozice znaku v řetězci, kde má být porovnání spuštěno.

Poznámka: Pole počáteční pozice je pozice znaku v řetězci pro porovnání, a tato pozice je vždy 37.

Program k volání
Název programu, který spouští příchozí program zpráv, který má být volán ke spuštění relace.

Program AMQCRC6Aje volán pro výchozího správce front. Tento program je dodáván s produktem IBM MQ for IBM i a nastavuje prostředí a poté volá příkaz AMQCRS6A.

Pro další správce front:

- Každý správce front má specifický program pro vyvolání LU 6.2 , který se nachází ve své knihovně. Tento program se nazývá AMQCRC6B a je automaticky generován při vytvoření správce front.
- Každý správce front vyžaduje, aby byla přidána specifická položka směrování s jedinečnými údaji o směrování. Tato data o směrování musí odpovídat názvu **transakčního programu** dodanému žádajícím systémem (viz Inicializace ukončení (Sender)).

Příklad je zobrazen v konfiguračním panelu komunikace LU 6.2 -zobrazení položek směrování:

```
Display Routing Entries
System:  MY400
Subsystem description:  QCMN      Status:  ACTIVE

Type options, press Enter.
5=Display details

Start
Opt  Seq Nbr  Program    Library    Compare Value   Pos
10   *RTGDTA           'QZSCSRVR'     37
20   *RTGDTA           '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 38. Konec komunikačního zařízení LU 6.2 -zahájený konec

V okně LU 6.2 communication setup panel-display routing entries, pořadové číslo 90 představuje výchozího správce front a poskytuje kompatibilitu s konfiguracemi z předchozích vydání (tj. V3R2, V3R6, V3R7a V4R2) produktu IBM MQ for IBM i. Tato vydání umožňují pouze jednoho správce front. Pořadová čísla 92 a 94 představují dva další správce front s názvem ALPHA a BETA, které jsou vytvořeny s knihovnami QMALPHA a QMBETA.

Poznámka: Pro každého správce front můžete použít více směrovacích dat pomocí různých směrovacích dat, více než jeden záznam směrování. Tyto záznamy dávají možnost různých priorit práce v závislosti na použitých třídách.

Třída
Název a knihovna třídy použité pro kroky spuštěné prostřednictvím tohoto směrovacího záznamu. Třída definuje atributy běhového prostředí směrovacího kroku a uvádí prioritu úlohy. Musí být uvedena odpovídající položka třídy. Použijte například příkaz WRKCLS k zobrazení existujících tříd nebo pro vytvoření třídy. Další informace o správě pracovních požadavků ze vzdálených logických jednotek LU 6.2 jsou k dispozici v příručce *IBM i Programming: Work Management Guide*.

Poznámka k produktu Work Management

Úloha AMQCRS6A nemůže využít výhod normálních funkcí správy činnosti produktu IBM i , které jsou zdokumentovány v tématu Správa činnosti systému , protože není spuštěna stejným způsobem jako ostatní úlohy produktu IBM MQ . Chcete-li změnit vlastnosti běhového prostředí úloh příjemce LU62 , můžete provést jednu z následujících změn:

- Upravte popis třídy uvedený v záznamu směrování pro úlohu AMQCRS6A .
- Změna popisu úlohy v záznamu komunikace

Další informace o konfiguraci komunikačních úloh najdete v příručce *IBM i Programming: Work Management Guide* .

Konfigurace klastru správce front

Klastry poskytují 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 koncepce klastrování najdete v tématu Klastry.

Když navrhujete klastr správců front, musíte provést některá rozhodnutí. Viz Příklady klastrů a Navrhování klastrů.

Související úlohy

“Přesun definice tématu klastru do jiného správce front” na stránce 389
Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Související odkazy

Odstranit téma

Definování komponent klastru

Klastry se skládají z správců front, kanálů klastru a front klastru. Můžete definovat fronty klastru a upravit některé aspekty výchozích objektů klastru. Můžete získat informace o konfiguraci a stavu o automaticky definovaných kanálech a o vztazích mezi jednotlivými kanály odesílatele klastru a přenosové fronty.

Informace o definování jednotlivých komponent klastru najdete v následujících dílčích tématech:

Související pojmy

Komponenty klastru

Kanály klastru

Související úlohy

Definování témat klastru

“Nastavení nového klastru” na stránce 277
Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

“Přidání správce front do klastru” na stránce 288
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí jedné přenosové fronty klastru `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Definování front klastru

Fronta klastru je fronta, jejímž hostitelem je správce front klastru, a která je dostupná ostatním správcům front v klastru.Definujte frontu klastru jako lokální frontu ve správci front klastru, kde je fronta hostována. Uveďte název klastru, do kterého fronta patří.

Následující příklad ukazuje příkaz **runmqsc** k definování fronty klastru s volbou `CLUSTER` :

```
DEFINE QLOCAL(Q1) CLUSTER(SALES)
```

Definice fronty klastru se oznamuje ostatním správcům front v klastru. Ostatní správci front v klastru mohou vkládat zprávy do fronty klastru, aniž by potřebovali odpovídající definici vzdálené fronty. Fronta klastru může být oznámena ve více než jednom klastru pomocí seznamu názvů klastrů.

Po oznámení fronty může každý správce front v klastru do ní vkládat zprávy. Chcete-li správce front vložit zprávu, musí z úplných úložišť zjistit, kdo je hostitelem této fronty. Pak přidá do zprávy informace o 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 bude více než jeden správce front hostitelem instance stejné fronty klastru. Ujistěte se, že všechny zprávy v posloupnosti jsou odeslány do stejné instance fronty. Řadu zpráv můžete svázat do konkrétní fronty pomocí volby `MQOO_BIND_ON_OPEN` na volání `MQOPEN` .

Přenosové fronty klastru

Správce front může ukládat zprávy pro ostatní správce front z klastru do více přenosových front. Správce front můžete nakonfigurovat tak, aby ukládal zprávy do více přenosových front klastru, dvěma různými způsoby. 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 se umístí před odesláním do přenosové fronty klastru. Kanál odesílatele klastru přenáší zprávy z přenosové fronty klastru do kanálů příjemce klastru v jiných správcích front. Při výchozím nastavení má jedna systémem definovaná přenosová fronta klastru všechny zprávy, které mají být přeneseny do jiných správců front klastru. Fronta se nazývá SYSTEM.CLUSTER.TRANSMIT.QUEUE. Správce front, který je součástí klastru, může odesílat zprávy na tuto přenosovou frontu klastru libovolnému jinému správci front ve stejném klastru.

Definice pro jednu frontu SYSTEM.CLUSTER.TRANSMIT.QUEUE je standardně vytvářena ve všech správnic správce front kromě z/OS. z/OS V systému z/OSmůže být definice definována s dodaným vzorkem **CSQ4INSX**.

Správce front můžete nakonfigurovat tak, aby přenášels zprávy do jiných klastrovaných správců front používajících více přenosových front. Další přenosové fronty klastru můžete definovat ručně, nebo správce front automaticky vytvořit fronty.

Chcete-li, aby byly fronty vytvořeny automaticky správcem front, změňte atribut správce front DEFCLXQ z SCTQ na CHANNEL. Výsledkem je vytvoření jednotlivé přenosové fronty klastru pro každý odesílací kanál klastru, který je vytvořen. Přenosové fronty jsou vytvářeny jako trvalé dynamické fronty z modelové fronty SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE. Název každé trvalé dynamické fronty je SYSTEM.CLUSTER.TRANSMIT. *ChannelName*. Název odesílacího kanálu klastru, ke kterému je přidružena trvalá přenosová fronta dynamického klastru, je nastavena v atributu lokální přenosové fronty CLCHNAME. Zprávy pro vzdálené klastrované správce front se umísťují do trvalé přenosové fronty dynamického klastru pro přidružený odesílací kanál klastru, spíše než na SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Chcete-li vytvořit přenosové fronty klastru ručně, vytvořte lokální frontu s atributem USAGE nastaveným na hodnotu XMITQa atribut CLCHNAME je nastaven na generický název kanálu, který se interpretuje jako jeden nebo více odesílacích kanálů klastru; viz ClusterChannelNázev. Pokud vytvoříte přenosové fronty klastru ručně, máte možnost přidružit přenosovou frontu jedním odesílacím kanálem klastru nebo s více odesílacími kanály klastru. Atribut CLCHNAME je generický název, což znamená, že v názvu můžete umístit více zástupných znaků, "*".

S výjimkou počátečních odesílacích kanálů klastru, které vytváříte ručně pro připojení správce front k úplnému úložišti, jsou odesílací kanály klastru vytvářeny automaticky. Jsou vytvořeny automaticky, když existuje zpráva pro přenos do správce front klastru. Jsou vytvořeny se stejným názvem jako název přijímacího kanálu klastru, který přijímá zprávy klastru pro tento konkrétní klastr v cílovém správci front.

Pokud postupujete podle konvence pojmenování pro kanály příjemce klastru, je možné definovat generickou hodnotu pro CLCHNAME , která filtruje různé druhy zpráv klastru do různých přenosových front. Pokud například postupujete podle konvence pojmenování pro přijímací kanály klastru produktu *ClusterName*. *QmgrName*, pak generické jméno *ClusterName*.* filtruje zprávy pro různé klastry v různých přenosových frontách. Musíte definovat přenosové fronty ručně a nastavit CLCHNAME v každé přenosové frontě na *ClusterName*.*.

Změny přidružení přenosových front klastru k odesílacím kanálům klastru nepřijímají okamžitý účinek. Momentálně přidružená přenosová fronta, kterou kanál odesílatele klastru obsluhuje, může obsahovat zprávy, které jsou v procesu přenosu kanálem odesílatele klastru. Pouze pokud žádné zprávy v aktuálně

přidružené přenosové frontě nejsou zpracovávány kanálem odesílatele klastru, může správce front změnit přidružení odesílacího kanálu klastru s jinou přenosovou frontou. K tomu může dojít buď v situaci, kdy žádné zprávy nezůstanou v přenosové frontě ke zpracování kanálem odesílatele klastru, nebo když je zpracování zpráv pozastaveno a odesílací kanál klastru nemá žádné zprávy "in-flight" . Pokud k tomu dojde, všechny nezpracované zprávy pro kanál odesílatele klastru jsou přeneseny do nově přidružené přenosové fronty a přidružení kanálu odesílatele klastru se změní.

Můžete vytvořit definici vzdálené fronty, která bude interpretována jako přenosová fronta klastru. V definici se správce front QMX nachází ve stejném klastru jako lokální správce front a že neexistuje žádná přenosová fronta, QMX.

```
DEFINE QREMOTE(A) RNAME(B) RQMNAME(QMX)
```

Během rozpoznání názvu fronty má přenosová fronta klastru přednost před výchozí přenosovou frontou. Zpráva umístěná do produktu A je uložena v přenosové frontě klastru a poté odeslána do vzdálené fronty B v systému QMX.

Správci front mohou také komunikovat s ostatními správci front, kteří nejsou součástí klastru. Kanály a přenosové fronty je třeba definovat do druhého správce front stejným způsobem jako v prostředí s rozděleným frontami.

Poznámka: Aplikace musí zapisovat do front, které se interpretují do přenosové fronty klastru, a nesmí zapisovat přímo do přenosové fronty klastru.

Automatická definice vzdálených front

Správce front v klastru nepotřebuje definici vzdálené fronty pro vzdálené fronty v klastru. Správce front klastru vyhledá umístění vzdálené fronty z úplného úložiště. Přidává informace o směrování do zprávy a vkládá je do přenosové fronty klastru. Produkt IBM MQ automaticky vytvoří definici ekvivalentní definiční definici vzdálené fronty, aby mohla být zpráva odeslána.

Automaticky vytvořenou definici vzdálené fronty nelze změnit ani odstranit. Nicméně pomocí příkazu DISPLAY QUEUE **runmqsc** s atributem CLUSINFO můžete zobrazit všechny lokální fronty ve správci front i všechny fronty klastru, včetně front klastru ve vzdálených správcích front. Příklad:

```
DISPLAY QUEUE(*) CLUSINFO
```

Související pojmy

Fronty klastru

Související odkazy

Název ClusterChannel(MQCHAR20)

Práce s automaticky definovanými kanály odesílatele klastru

Po zavedení správce front do klastru provedením počátečních definic CLUSSDR a CLUSRCVR produkt IBM MQ při požadavku na přesun zpráv do jiného správce front v klastru automaticky provede další definice kanálů odesílatele klastru. Můžete zobrazit informace o automaticky definovaných odesílacích kanálech klastru, ale nemůžete je upravit. Chcete-li upravit jejich chování, můžete použít uživatelskou proceduru automatické definice kanálu.

Než začnete

Úvod do automaticky definovaných kanálů najdete v tématu Automaticky definované kanály odesílatele klastru.

Informace o této úloze

Automaticky definované kanály odesílatele klastru jsou vytvořeny klastrem jako a v případě potřeby a zůstanou aktivní, dokud nebudou ukončeny pomocí normálních pravidel pro odpojení.

Odesílací kanály klastru (CLUSSDR) mohou být automaticky definovány jak pro přesun aplikačních zpráv, tak pro interní administrativní zprávy klastru. Například v klastru Publikování/odběr (jeden ve kterém bylo definováno klastrované téma) lze definovat kanály mezi dílčími úložišti a povolit výměnu stavu 'proxy odběry'. Není-li vyžadováno (neaktivní) po delší dobu, jsou automaticky definované CLUSSDR odebírány z mezipaměti dílčího úložiště informací o klastru a nejsou nadále viditelné pro daného správce front.

Multi V systému Multiplatformsnení produkt OAM (správce oprávnění k objektu) informován o existenci automaticky definovaných odesílacích kanálů klastru. Pokud zadáte příkazy **start**, **stop**, **ping**, **reset**nebo **resolve** na automaticky definovaný odesílací kanál klastru, zkontroluje produkt OAM, zda máte oprávnění provádět stejnou akci u odpovídajícího přijímacího kanálu klastru.

z/OS V systému z/OSmůžete zabezpečit automaticky definovaný kanál odesílatele klastru stejným způsobem jako kterýkoli jiný kanál.

Procedura

- Zobrazí informace o automaticky definovaných kanálech pro daného správce front klastru.

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

  ```
  DISPLAY CLUSQMGR(qMgrName)
  ```

- Zobrazte stav automaticky definovaného kanálu pro danou položku CLUSRCVR.

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

  ```
  DISPLAY CHSTATUS(channelname)
  ```

- Chcete-li upravit chování automaticky definovaného kanálu, použijte proceduru automatické definice kanálu.

  Uživatelská procedura automatické definice kanálu produktu IBM MQ můžete použít, chcete-li napsat uživatelský ukončovací program pro přizpůsobení kanálu odesílatele klastru nebo kanálu příjemce klastru. Například můžete použít uživatelskou proceduru pro automatickou definici kanálu v klastrovaném prostředí, abyste provedli libovolnou z následujících úprav:

  - Definice komunikačních prostředků, tj. názvy protokolů SNA LU6.2 .
  - Přidejte nebo odeberte jiné uživatelské procedury, např. uživatelské procedury pro zabezpečení zprávy.
  - Změňte názvy uživatelských procedur kanálu.

    Název uživatelské procedury kanálu CLUSSDR je automaticky generován z definice kanálu CLUSRCVR , a proto nemusí být vhodný pro vaše potřeby-zejména, pokud jsou dva konce kanálu na různých platformách.

    Formát názvů uživatelských procedur se liší na různých platformách. Příklad:

    - z/OS Na platformě z/OS je formát parametru SCYEXIT (*název uživatelské procedury zabezpečení*) SCYEXIT('SECEXIT') .
    - Windows Na platformách Windows je formát parametru SCYEXIT (*název uživatelské procedury zabezpečení*) SCYEXIT(' *drive*:*path**library* (secexit)') .

    Poznámka: z/OS Není-li k dispozici žádná uživatelská procedura automatické definice kanálu, správce front produktu z/OS odvozuje název uživatelské procedury kanálu CLUSSDR z definice kanálu CLUSRCVR na druhém konci kanálu. Chcete-li odvodit název uživatelské procedury z/OS z názvu, který není názvemz/OS , použije se následující algoritmus:

    - Názvy uživatelských procedur v systému Multiplatforms mají obecný tvar *cesta*/*knihovna* (*funkce*).

- Je-li přítomen *funkce* , použije se až osm znaků.
- Jinak se použije až osm znaků *knihovny* .

Příklad:

- `/var/mqm/exits/myExit.so(MsgExit)` převádí na `MSGEXIT`
- `/var/mqm/exits/myExit` převádí na `MYEXIT`
- `/var/mqm/exits/myExit.so(ExitLongName)` převádí na `EXITLONG`

- Pro správce front starší než IBM WebSphere MQ 7nastavte atribut **PROPCTL** na hodnotu `NONE`.

  Každý automaticky definovaný kanál odesílatele klastru je založen na příslušném přijímacím kanálu klastru. Před IBM WebSphere MQ 7nemá kanál příjemce klastru atribut **PROPCTL** , takže tento atribut je proto nastaven na hodnotu `COMPAT` v automaticky definovaném kanálu odesílatele klastru.

  Pokud klastr potřebuje použít produkt **PROPCTL** k odebrání záhlaví aplikací, například RFH2 , z zpráv, které pochází od správce front produktu IBM WebSphere MQ 7 nebo novějšího do správce front v dřívější verzi produktu IBM MQ, je nutné zadat uživatelskou proceduru s automatickou definicí kanálu s hodnotou **PROPCTL** na hodnotu `NONE`.

- Použijte atribut kanálu `LOCLADDR` k řízení aspektů adresování.
  - Chcete-li povolit odchozí kanál (TCP) pro použití konkrétní adresy IP, portu nebo rozsahu portů, použijte atribut kanálu `LOCLADDR`. To je užitečné tehdy, máte-li více než jednu síťovou kartu a chcete, aby kanál používal pro odchozí komunikaci určitou specifickou síťovou kartu.
  - Chcete-li určit virtuální adresu IP v kanálu `CLUSSDR` , použijte adresu IP z `LOCLADDR` na ručně definovaném `CLUSSDR`. Chcete-li určit rozsah portů, použijte rozsah portů od `CLUSRCVR`.
  - Pokud klastr potřebuje použít `LOCLADDR` k získání odchozích komunikačních kanálů pro připojení k určité adrese IP, můžete zapsat uživatelskou proceduru s automatickou definicí kanálu, aby vynutila hodnotu `LOCLADDR` do libovolného ze svých automaticky definovaných kanálů `CLUSSDR` . Je třeba ji zadat také v ručně definovaném kanálu `CLUSSDR` .
  - Zadejte číslo portu nebo rozsah portů v souboru `LOCLADDR` kanálu `CLUSRCVR` , pokud chcete, aby všichni správci front v klastru používali pro všechny své odchozí komunikace specifický port nebo rozsah portů.

  Poznámka: Nevkládejte adresu IP do pole `LOCLADDR` kanálu `CLUSRCVR` , pokud se všichni správci front nenachází na stejném serveru. Adresa IP `LOCLADDR` je předána do automaticky definovaných kanálů `CLUSSDR` všech správců front, které se připojují pomocí kanálu `CLUSRCVR` .

  Multi V systému Multiplatformsmůžete nastavit výchozí hodnotu lokální adresy, která se použije pro všechny odesílací kanály, pro které není definována lokální adresa. Výchozí hodnota je definována nastavením proměnné prostředí MQ_LCLADDR před spuštěním správce front. Formát hodnoty odpovídá hodnotě atributu MQSC `LOCLADDR`.

Související odkazy

Lokální adresa (LOCLADDR)

Práce s výchozími objekty klastru

Výchozí definice kanálů můžete změnit stejným způsobem jako v libovolné jiné definici kanálu spuštěním příkazů MQSC nebo PCF. Neměňte výchozí definice fronty, kromě `SYSTEM.CLUSTER.HISTORY.QUEUE`.

Úplný seznam těchto objektů najdete v tématu Výchozí objekty klastru. Následující seznam obsahuje pouze ty objekty, které můžete změnit.

`SYSTEM.CLUSTER.HISTORY.QUEUE`
Každý správce front v klastru má lokální frontu s názvem `SYSTEM.CLUSTER.HISTORY.QUEUE`. Produkt `SYSTEM.CLUSTER.HISTORY.QUEUE` se používá k ukládání historie informací o stavu klastru pro účely služby.

Ve výchozím nastavení objektu je parametr SYSTEM.CLUSTER.HISTORY.QUEUE nastaven na hodnotu PUT (ENABLED). Chcete-li potlačit shromažďování historie, změňte nastavení na hodnotu PUT (DISABLED).

SYSTEM.CLUSTER.TRANSMIT.QUEUE
Každý správce front má definici pro lokální frontu s názvem SYSTEM.CLUSTER.TRANSMIT.QUEUE. SYSTEM.CLUSTER.TRANSMIT.QUEUE je výchozí přenosová fronta pro všechny zprávy do všech front a správců front, kteří jsou v klastrech. Výchozí přenosovou frontu pro každý odesílací kanál klastru můžete změnit na SYSTEM.CLUSTER.TRANSMIT.*ChannelName*změnou atributu správce front DEFXMITQ z/OS , kromě na z/OS . Produkt SYSTEM.CLUSTER.TRANSMIT.QUEUEnelze odstranit. Používá se také k definování kontroly autorizace, zda je použita výchozí přenosová fronta, která se používá, SYSTEM.CLUSTER.TRANSMIT.QUEUE nebo SYSTEM.CLUSTER.TRANSMIT.*ChannelName*.

Související pojmy
Výchozí objekty klastru

Práce s přenosovými frontami klastru a odesílacími kanály klastru
Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru. V libovolném okamžiku je kanál odesílatele klastru asociován s jednou přenosovou frontou. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizováno a transakční.

Spuštěním následujícího příkazu MQSC zobrazte přenosové fronty, ke kterým jsou kanály odesílatele klastru přidruženy:

```
DISPLAY CHSTATUS(*) WHERE(CHLTYPE EQ CLUSSDR)
```

```
AMQ8417: Display Channel Status details.
CHANNEL(TO.QM2)          CHLTYPE(CLUSSDR)
CONNAME(9.146.163.190(1416))    CURRENT
RQMNAME(QM2)             STATUS(STOPPED)
SUBSTATE( )            XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

Přenosová fronta zobrazená v uloženém stavu kanálu zastaveného kanálu odesílatele klastru se může změnit, jakmile se kanál spustí znovu. “Výběr výchozích přenosových front podle kanálů odesílatele klastru” na stránce 272 popisuje proces výběru výchozí přenosové fronty; “Výběr ručně definovaných přenosových front pomocí kanálů odesílatele klastru” na stránce 272 popisuje proces výběru ručně definované přenosové fronty.

Když některý odesílací kanál klastru začne znovu zkontrolovat své přidružení k přenosovým frontám. Pokud se změní konfigurace přenosových front nebo výchozí nastavení správce front, může kanál znovu asociovat s jinou přenosovou frontou. Pokud se kanál restartuje s jinou přenosovou frontou jako výsledek změny konfigurace, provede se proces přenosu zpráv do nově přidružené přenosové fronty. “Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje” na stránce 273 popisuje proces přenosu odesílacího kanálu klastru z jedné přenosové fronty do jiné.

Chování odesílacích kanálů klastru se liší od kanálů odesílatele a serveru. Zůstávají přidruženy ke stejné přenosové frontě, dokud se nezmění atribut kanálu **XMITQ** . Pokud změníte atribut přenosové fronty na odesílacím kanálu nebo na kanálu serveru a restartujete jej, nebudou zprávy přeneseny z původní přenosové fronty do nové.

Další rozdíl mezi odesílanými kanály klastru a kanály odesílatele nebo serveru znamená, že více odesílacích kanálů klastru může otevřít přenosovou frontu klastru, ale může normální přenosovou frontu otevřít pouze jeden odesílací kanál nebo kanál serveru. Do IBM WebSphere MQ 7.5klastrová spojení sdíleli jednu přenosovou frontu klastru, SYSTEM.CLUSTER.TRANSMIT.QUEUE. Počínaje produktem IBM WebSphere MQ 7.5 máte možnost volby odesílacího kanálu klastru, který nesdílí přenosové fronty. Exkluzivita není vynucena; je výsledkem konfigurace. Cestu ke zprávě lze konfigurovat v klastru tak, aby nesdílela žádné přenosové fronty nebo kanály se zprávami, které tečou mezi ostatními aplikacemi. Viz

Clustering: Planning how to configure cluster transmission queues a “Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 322.

Výběr výchozích přenosových front podle kanálů odesílatele klastru

Přenosová fronta klastru je buď systémová předvolená fronta, s názvem, který začíná SYSTEM.CLUSTER.TRANSMIT, nebo ručně definovanou frontou. Odesílací kanál klastru je asociován s přenosovou frontou klastru jedním ze dvou způsobů: výchozím mechanizmem přenosové fronty klastru nebo ruční konfigurací.

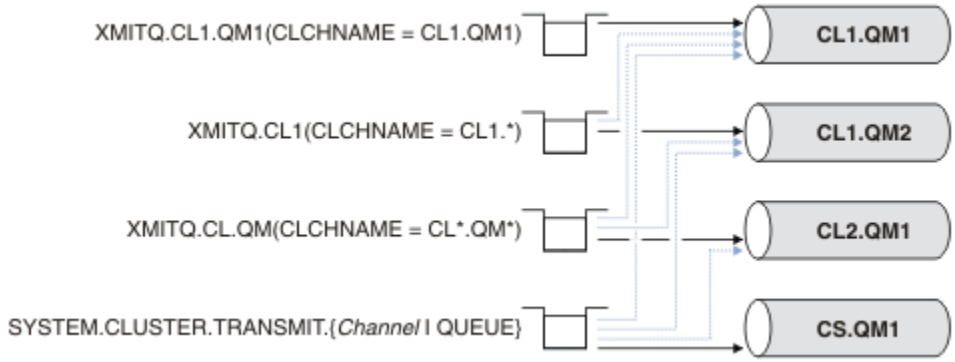
Výchozí přenosová fronta klastru je nastavena jako atribut správce front, **DEFCLXQ**. Jeho hodnota je buď SCTQ , nebo CHANNEL. Noví a migrovaní správci front jsou nastavovali na hodnotu SCTQ. Tuto hodnotu můžete změnit na CHANNEL.

Je-li nastavena hodnota SCTQ , je výchozí přenosová fronta klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE. Tuto frontu může otevřít každý odesílací kanál klastru. Odesílací kanály klastru, které otevírají frontu, jsou ty, které nejsou přidruženy k ručně definovaným přenosovým frontám klastru.

Je-li nastavena volba CHANNEL , může správce front vytvořit samostatnou trvalou dynamickou přenosovou frontu pro každý odesílací kanál klastru. Každá fronta má název SYSTEM.CLUSTER.TRANSMIT. *ChannelName* a je vytvořena z modelové fronty SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE. Každý odesílací kanál klastru, který není přidružen k ručně definované přenosové frontě klastru, je přidružen k frontě pro přenosovou frontu trvalého dynamického klastru. Fronta je vytvořena správcem front, vyžaduje-li pro cíl klastru obsluhovaný tímto odesílacím kanálem klastru samostatnou přenosovou frontu klastru a žádná fronta neexistuje.

Některá místa určení klastru mohou být obsluhována odesílacími kanály klastru přidruženými k ručně definovaným frontám přenosu a ostatním prostřednictvím výchozí fronty nebo front. V přidružení odesílacích kanálů klastru s přenosovými frontami mají ručně definované přenosové fronty vždy přednost před výchozími přenosovými frontami.

Pořadí přenosových front klastru je ilustrováno v Obrázek 39 na stránce 272. Jediný odesílací kanál klastru, který není přidružený k ručně definované přenosové frontě klastru, je CS.QM1. Nevztahuje se k ručně definované přenosové frontě, protože žádný z názvů kanálů v atributu **CLCHNAME** přenosových front neodpovídá CS.QM1.



Obrázek 39. Priorita přenosové fronty/klastru-priorita odesílatele

Výběr ručně definovaných přenosových front pomocí kanálů odesílatele klastru

Ručně definovaná fronta má atribut **USAGE** atributu přenosové fronty nastavený na hodnotu XMITQa atribut názvu kanálu klastru **CLCHNAME** je nastaven na specifický nebo generický název kanálu.

Pokud se název v atributu fronty produktu **CLCHNAME** shoduje s názvem kanálu odesílatele klastru, kanál je přidružen ke frontě. Název je buď přesná shoda, pokud název neobsahuje žádné zástupné znaky, nebo to nejlepší shodu, pokud název obsahuje zástupné znaky.

Pokud se definice **CLCHNAME** ve více přenosových frontách shodují se stejným kanálem odesílatele klastru, definice se mají překrývat. Chcete-li vyřešit nejednoznačnost, existuje pořadí priorit mezi shodami. Přesná shoda má vždy přednost. Obrázek 39 na stránce 272 zobrazuje přidružení mezi přenosovou frontou a odesílacími kanály klastru. Černé šipky ukazují skutečné svazy a šedé šípy, potenciální svazy. Pořadí priorit přenosových front v produktu Obrázek 39 na stránce 272 je následující:

XMITQ.CL1.QM1
: Přenosová fronta `XMITQ.CL1.QM1` má svůj atribut **CLCHNAME** nastaven na `CL1.QM1`. Definice atributu **CLCHNAME** , `CL1.QM1`, nemá žádné zástupné znaky a má přednost před všemi ostatními atributy `CLCHNAME` definovanými v jiných přenosových frontách, které se shodují se zástupnými znaky. Správce front uloží jakoukoli zprávu klastru, která má být přenesena kanálem odesílatele klastru `CL1.QM1` do přenosové fronty produktu `XMITQ.CL1.QM1` . Jediná výjimka je, pokud má více přenosových front svůj atribut **CLCHNAME** nastaven na `CL1.QM1`. V takovém případě správce front ukládá zprávy pro odesílací kanál klastru `CL1.QM1` v jakékoli z těchto front. Vybírá frontu libovolně, když se spustí kanál. Je-li kanál znovu spuštěn, může být vybrána jiná fronta.

XMITQ.CL1
: Přenosová fronta `XMITQ.CL1` má svůj atribut **CLCHNAME** nastaven na `CL1.*`. Definice atributu **CLCHNAME** , `CL1.*`, má jeden koncový zástupný znak, který odpovídá názvu libovolného kanálu odesílatele klastru, který začíná na `CL1.`. Správce front uloží všechny zprávy klastru, které mají být přeneseny libovolným odesílacím kanálem klastru, jehož název začíná na `CL1.` v přenosové frontě `XMITQ.CL1`, pokud neexistuje přenosová fronta se specifičtější shodou, jako je fronta `XMITQ.CL1.QM1`. Jeden koncový zástupný znak učiní definici méně specifickou než definici bez zástupných znaků a specifičtější než definice s více zástupnými znaky, nebo zástupné znaky, za kterými následují další koncové znaky.

XMITQ.CL.QM
: `XMITQ.CL.QM` je název přenosové fronty se svým atributem **CLCHNAME** nastaveným na `CL*.QM*`. Definice produktu `CL*.QM*` má dva zástupné znaky, které se shodují s názvem kanálu odesílatele klastru, který začíná na `CL.`, a to buď zahrnuje, nebo končí na `QM`. Shoda je méně specifická než shoda s jedním zástupným znakem.

SYSTEM.CLUSTER.TRANSMIT. *channelName*|QUEUE
: Pokud nemá žádná přenosová fronta atribut **CLCHNAME** , který odpovídá názvu kanálu odesílatele klastru, který má být používán správcem front, pak správce front použije výchozí přenosovou frontu klastru. Výchozí přenosová fronta klastru je buď přenosová fronta klastru jednoho systému, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`, nebo přenosová fronta klastru systému, kterou správce front vytvořil pro specifický odesílací kanál klastru, `SYSTEM.CLUSTER.TRANSMIT.` *channelName*. Která fronta je výchozí, závisí na nastavení atributu správce front **DEFXMITQ** .

Tip: Pokud nemáte jasnou potřebu překrývajících se definic, vyhnete se jim, protože mohou vést ke složitým konfiguracím, které jsou těžko pochopitelné.

Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje

Chcete-li změnit přidružení odesílacích kanálů klastru ke frontám přenosu klastru, změňte parametr **CLCHNAME** v libovolné přenosové frontě nebo parametru správce front **DEFCLXQ** kdykoli. Nic se nestane okamžitě. Změny se vyskytnou pouze při spuštění kanálu. Když se spustí, bude kontrolovat, zda pokračovat ve směrování zpráv ze stejné přenosové fronty. Tři druhy změn mění přidružení odesílacího kanálu klastru k přenosové frontě.

1. Při předefinování parametru **CLCHNAME** přenosové fronty je kanál odesílatele klastru v současné době přidružen k méně specifickému nebo mezerovém stavu, nebo při zastavení kanálu se odstraní přenosové fronty klastru.

   Pro název kanálu by nyní mohla být lepší shoda s jinou přenosovou frontou klastru. Nebo, pokud se žádné jiné přenosové fronty neshodují s názvem kanálu odesílatele klastru, přidružení se musí vrátit k výchozí přenosové frontě.
2. Předefinování parametru **CLCHNAME** jakékoli jiné přenosové fronty klastru nebo přidání přenosové fronty klastru.

Parametr **CLCHNAME** jiné přenosové fronty může nyní být lepší pro kanál odesílatele klastru, než je odesílací kanál, se kterým je aktuálně asociován odesílací kanál klastru. Je-li odesílací kanál klastru momentálně přidružen k výchozí přenosové frontě klastru, může být přidružen k ručně definované přenosové frontě klastru.

3. Je-li odesílací kanál klastru aktuálně přidružen k výchozí přenosové frontě klastru, změňte parametr správce front **DEFCLXQ** .

Změní-li se přidružení odesílacího kanálu klastru, změní-li se kanál, přepne se do nové přenosové fronty. Během přepínače se ujistí, že žádné zprávy nejsou ztraceny. Zprávy se přenášejí do nové přenosové fronty v pořadí, ve kterém bude kanál přenášet zprávy do vzdáleného správce front.

Zapamatujte si: Při předávání zpráv v klastru je třeba do skupin vložit zprávy, které zajistí, že zprávy, které musí být doručovány v pořadí, jsou doručovány v pořadí. Ve výjimečných případech může dojít k nedostatku zpráv v klastru.

Proces přepnutí probíhá přes následující transakční kroky. Je-li proces přepnutí přerušen, aktuální transakční krok se obnoví znovu, když se kanál znovu spustí.

Krok 1-Zpracování zpráv z původní přenosové fronty
Odesílací kanál klastru je přidružen k nové přenosové frontě, kterou může sdílet s ostatními odesílacími kanály klastru. Zprávy pro kanál odesílatele klastru budou nadále umístěny do původní přenosové fronty. Přechodný proces přepnutí přenese zprávy z původní přenosové fronty do nové přenosové fronty. Odesílací kanál klastru předává zprávy z nové přenosové fronty do přijímacího kanálu klastru. Stav kanálu ukazuje odesílací kanál klastru, který je stále přidružen ke staré přenosové frontě.

Proces přepnutí také pokračuje v přenášení nově příchozích zpráv. Tento krok pokračuje, dokud počet zbývajících zpráv, které se mají postoupit procesem přepnutí, dosáhne nulové hodnoty. Když počet zpráv dosáhne nuly, procedura se přesune na krok 2.
Během kroku 1 se zvyšuje aktivita disku pro kanál. Trvalé zprávy jsou potvrzeny z první přenosové fronty a do druhé přenosové fronty. Tato disková aktivita je navíc k potvrzeným zprávám, když jsou umístěny do přenosové fronty a odstraněny z přenosové fronty jako součást přenosu zpráv normálně. V ideálním případě se během procesu přepínání nepřijímají žádné zprávy, takže přechod se může uskutečnit co nejrychleji. Pokud zprávy dorazí, zpracují se procesem přepnutí.

Krok 2-Zpracovat zprávy z nové přenosové fronty
Jakmile žádné zprávy zůstanou v původní přenosové frontě pro odesílací kanál klastru, budou nové zprávy umístěny přímo do nové přenosové fronty. Stav kanálu ukazuje, že kanál odesílatele klastru je přidružen k nové přenosové frontě. Do protokolu chyb správce front se zapíše následující zpráva: " AMQ7341 `Přenosová fronta pro kanál` *`ChannelName`* `je` *`QueueName`* ."

Více přenosových front klastru a atributů přenosové fronty klastru

Máte možnost volby postoupení zpráv klastru různým správcům front, které ukládají zprávy do jedné přenosové fronty klastru nebo do více front. S jednou frontou máte jednu sadu atributů přenosové fronty klastru k nastavení a dotazu; s více frontami máte více sad. Pro některé atributy je výhodou více sad: například dotaz na hloubku fronty informuje o tom, kolik zpráv čeká na postoupení prostřednictvím jedné nebo více kanálů, nikoli všemi kanály. Pro další atributy je v nevýhodě více sad: například pravděpodobně nechcete konfigurovat stejná přístupová oprávnění pro každou přenosovou frontu klastru. Z tohoto důvodu jsou přístupová oprávnění vždy kontrolována proti profilu pro produkt `SYSTEM.CLUSTER.TRANSMIT.QUEUE`a nikoli pro profily pro konkrétní přenosovou frontu klastru. Chcete-li aplikovat podrobnější kontroly zabezpečení, prostudujte si téma Řízení přístupu a více přenosových front klastru.

Více odesílacích kanálů klastru a více přenosových front

Správce front uloží zprávu do přenosové fronty klastru před tím, než ji předá na odesílací kanál klastru. Vybere kanál odesílatele klastru, který je připojen k místu určení pro zprávu. Může jít o výběr odesílacích kanálů klastru, které se všechny připojují ke stejnému cíli. Místo určení může být stejná fyzická fronta připojená více odesílacími kanály klastru k jednomu správci front. Místo určení může být také

mnoho fyzických front se stejným názvem fronty, které jsou hostované na různých správcích front ve stejném klastru. Pokud existuje volba kanálů odesílatele klastru připojených k místu určení, algoritmus vyrovnávání pracovní zátěže si zvolí jeden z nich. Volba závisí na řadě faktorů. Další informace naleznete v tématu Algoritmus správy pracovní zátěže klastru.

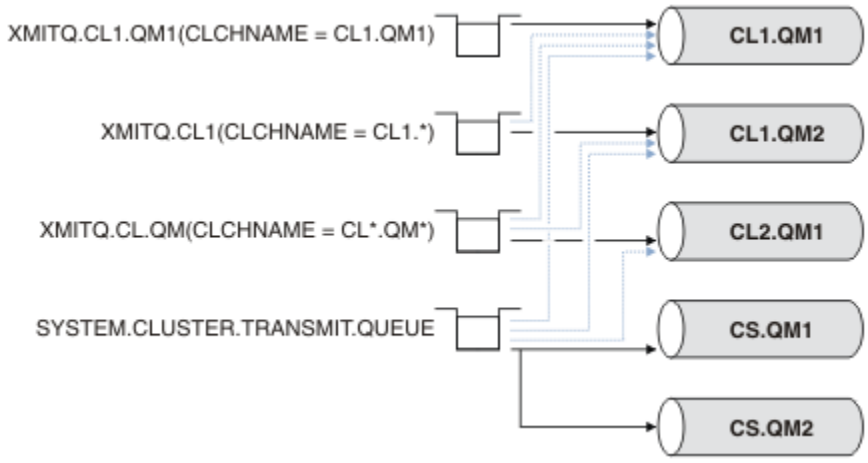
V systémech Obrázek 40 na stránce 275, `CL1.QM1`, `CL1.QM2` a `CS.QM1` jsou všechny kanály, které mohou vést ke stejnému cíli. Pokud například definujete `Q1` v `CL1` na `QM1` a `QM2` pak `CL1.QM1` a `CL1.QM2` obě poskytují přenosové cesty ke stejnému cíli, `Q1`, na dvou různých správcích front. Je-li kanál `CS.QM1` také v `CL1`, je to také kanál, který může přijmout zpráva pro `Q1` . Členství v klastru produktu `CS.QM1` může být definováno v seznamu názvů klastru, což je důvod, proč název kanálu neobsahuje v jeho konstrukci název klastru. V závislosti na parametrech vyrovnávání pracovní zátěže a v odesílající aplikaci mohou být některé zprávy pro `Q1` umístěny na každou přenosovou frontu, `XMITQ.CL1.QM1`, `XMITQ.CL1` a `SYSTEM.CLUSTER.TRANSMIT.CS.QM1`.

Pokud chcete oddělit provoz zpráv, takže zprávy pro stejné místo určení nesdílejí fronty nebo kanály se zprávami pro různá místa určení, musíte nejprve zvážit, jak rozdělit provoz na různé odesílací kanály klastru, a pak jak oddělit zprávy pro konkrétní kanál do jiné přenosové fronty. Klastrované fronty ve stejném klastru, ve stejném správci front, obvykle sdílejí stejné kanály klastru. Definování více přenosových front klastru samo o sobě nepostačuje k oddělení provozu zpráv klastru do různých front. Pokud neoddělíte zprávy pro různé cílové fronty na různých kanálech, budou zprávy sdílet stejnou přenosovou frontu klastru.

Přímočarým způsobem, jak oddělit kanály, které zprávy přijímají, je vytvořit více klastrů. V každém správci front v každém klastru definujte pouze jednu frontu klastru. Definujete-li pro každou kombinaci klastru a správce front jiný kanál příjemce klastru, zprávy pro každou frontu klastru nesdílejí kanál klastru se zprávami pro jiné fronty klastru. Definujete-li oddělené přenosové fronty pro kanály klastru, odesílající správce front ukládá zprávy pouze pro jednu frontu klastru v každé přenosové frontě. Pokud například chcete, aby dvě fronty klastru nesdílely prostředky, můžete je buď umístit do různých klastrů ve stejném správci front, nebo na různých správcích front ve stejném klastru.

Volba přenosové fronty klastru nemá vliv na algoritmus vyrovnávání pracovní zátěže. Algoritmus vyrovnávání pracovní zátěže si vybírá, který kanál odesílatele klastru má předat zprávu. Zpráva umístí zprávu do přenosové fronty, která je obsluhována daným kanálem. Je-li pro algoritmus vyrovnávání pracovní zátěže volán znovu, například pokud se kanál zastaví, může být schopen vybrat jiný kanál k předání zprávy. Pokud si zvolí jiný kanál a nový kanál předává zprávy z jiné přenosové fronty klastru, algoritmus vyrovnávání pracovní zátěže přenese zprávu do jiné přenosové fronty.

V produktu Obrázek 40 na stránce 275jsou k výchozí přenosové frontě systému přidruženy dva kanály odesílatele klastru `CS.QM1` a `CS.QM2`. Když algoritmus vyrovnávání pracovní zátěže ukládá zprávu v produktu `SYSTEM.CLUSTER.TRANSMIT.QUEUE`nebo v jiné přenosové frontě klastru, je název odesílacího kanálu klastru, který má předat zprávu, uložen do ID korelace zprávy. Každý kanál předává pouze ty zprávy, které odpovídají ID korelace s názvem kanálu.



Obrázek 40. Více odesílacích kanálů klastru

Pokud se produkt CS.QM1 zastaví, budou prozkoumány zprávy v přenosové frontě pro daný odesílací kanál klastru. Tyto zprávy, které mohou být předány jiným kanálem, jsou znovu zpracovány algoritmem vyrovnávání pracovní zátěže. Jejich ID korelace je resetováno na alternativní název kanálu odesílatele klastru. Je-li alternativní odesílací kanál klastru CS.QM2, zpráva zůstane na SYSTEM.CLUSTER.TRANSMIT.QUEUE. Je-li alternativní kanál CL1.QM1, algoritmus vyrovnávání pracovní zátěže přenese zprávu do produktu XMITQ.CL1.QM1. Jsou-li restartována odesílací kanál klastru, nové zprávy a zprávy, které nebyly označeny příznakem pro jiný odesílací kanál klastru, jsou znovu přeneseny kanálem.

Přidružení mezi přenosovými frontami a odesílacími kanály klastru můžete změnit na spuštěném systému. V přenosové frontě můžete změnit parametr **CLCHNAME** nebo změnit parametr správce front **DEFCLXQ** . Když se kanál, který je ovlivněn změnou restartů, spustí proces přepínání přenosové fronty, viz "Jak proces přepnout kanál odesílatele klastru do jiné přenosové fronty funguje" na stránce 273.

Proces přepnutí přenosové fronty se spustí, když se kanál restartuje. Proces vyvažování zátěže se spustí po zastavení kanálu. Tyto dva procesy mohou běžet paralelně.

Jednoduchý případ při zastavení kanálu odesílatele klastru nezpůsobí, že proces nového vyvažování klastru změní kanál odesílatele klastru, který má předat zprávy ve frontě. Tento případ se týká případu, kdy žádný jiný odesílací kanál klastru nemůže předat zprávy do správného místa určení. Pokud neexistuje alternativní odesílací kanál klastru k předání zpráv do místa určení, zprávy zůstanou pro stejný odesílací kanál klastru po zastavení kanálu odesílatele klastru označeny příznakem pro stejný kanál odesílatele klastru. Když se kanál spustí, pokud je přepínač v nevyřízeném stavu, přesune tyto zprávy do jiné přenosové fronty, kde jsou zpracovávány stejným odesílacím kanálem klastru.

Složenější případ je místo, kde více než jeden odesílací kanál klastru může zpracovávat některé zprávy do stejného cíle. Chcete-li aktivovat přepínač přenosové fronty, zastavte a znovu spusťte odesílací kanál klastru. V mnoha případech při restartování kanálu již algoritmus vyrovnávání pracovní zátěže přesunul zprávy z původní přenosové fronty do různých přenosových front obsluhovaných různými kanály odesílatele klastru. Do nové přenosové fronty zůstanou přeneseny pouze ty zprávy, které nelze předat jiným odesílacím kanálem klastru. V některých případech, je-li kanál restartován rychle, zůstávají některé zprávy, které mohou být přeneseny algoritmem vyrovnávání pracovní zátěže. V takovém případě jsou některé zbývající zprávy přepnuty procesem vyrovnávání pracovní zátěže a některým procesem přepnutí přenosové fronty.

Související pojmy

Kanály klastru

"Výpočet velikosti protokolu" na stránce 579
Odhadování velikosti protokolu, které správce front potřebuje.

Související úlohy

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

"Vytvoření dvou překrývajících se klastrů se správcem front brány" na stránce 312
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 290
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

"Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 319
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

"Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 322

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

Nastavení nového klastru

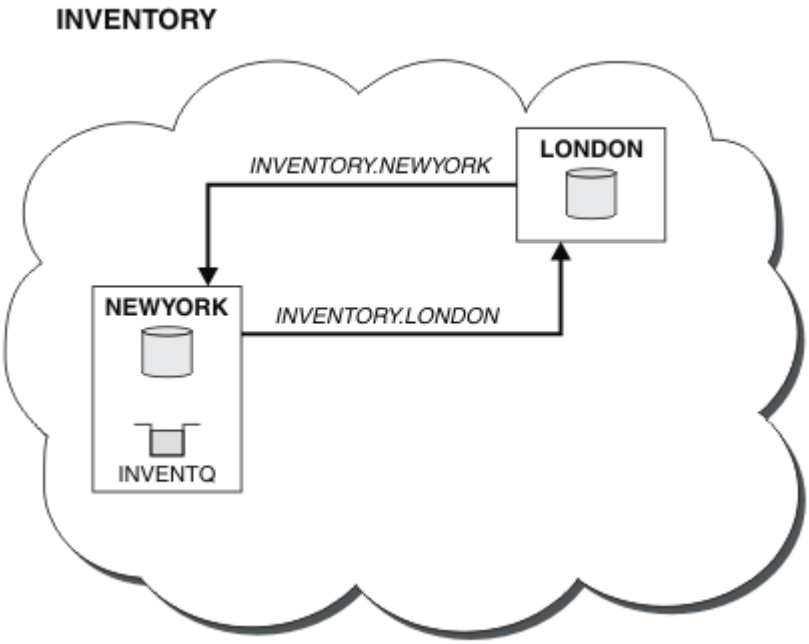
Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

Než začnete

- Místo následujících pokynů můžete pomocí jednoho z průvodců dodávaných s produktem IBM MQ Explorer vytvořit klastr podobný tomu, který vytvořil tato úloha. Klepněte pravým tlačítkem myši na složku Klastry správců front a poté klepněte na volbu **Nový** > **Klastr správců front**a postupujte podle pokynů uvedených v průvodci.
- Doplňující informace týkající se podpory pokynů k nastavení klastru najdete v tématu “Definování front klastru” na stránce 266, Kanály klastru a Listenery.

Informace o této úloze

Nastavujete novou síť IBM MQ pro úložiště řetězců. Obchod má dvě pobočky, jeden v Londýně a jeden v New Yorku. Data a aplikace pro každé úložiště jsou hostovány systémy, které spouštějí samostatné správce front. Dva správci front se nazývají LONDON a NEWYORK. Aplikace soupisu se spustí na systému v New Yorku, který je připojen ke správci front NEWYORK. Aplikace je řízena doručením zpráv ve frontě INVENTQ hostované serverem NEWYORK. Dva správci front, LONDON a NEWYORK, mají být propojeny v klastru s názvem INVENTORY , takže mohou oba vkládat zprávy do INVENTQ.



Tento klastr vypadá takto:

Každý správce front v klastru můžete nakonfigurovat tak, aby odesílal zprávy jiným správcům front v klastru pomocí různých přenosových front klastru.

Pokyny pro nastavení klastru se liší podle transportního protokolu, počtu přenosových front nebo platformy. Máte na výběr ze tří kombinací. Ověřovací procedura zůstane stejná pro všechny kombinace.

INVENTORY je malý klastr. Nicméně je to užitečné jako důkaz konceptu. Důležitým krokem při pochopení tohoto klastru je rozsah, který nabízí pro budoucí vylepšení.

Procedura

- “Nastavení klastru pomocí protokolu TCP/IP s jedinou přenosovou frontou na správce front” na stránce 278
- “Nastavení klastru v systému TCP/IP s použitím více přenosových front na jednoho správce front” na stránce 281
- “Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 284
- “Ověření klastru” na stránce 286

Související pojmy

Klastry

Porovnání klastrování a distribuovaných front

Komponenty klastru

Související úlohy

“Konfigurace klastru správce front” na stránce 265

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 jedinou přenosovou frontou na správce front

Jedná se o jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

Než začnete

Přehled klastru, který se vytváří, viz “Nastavení nového klastru” na stránce 277.

Atribut správce front, **DEFCLXQ**, musí být ponechán jako výchozí hodnota SCTQ.

Informace o této úloze

Chcete-li nastavit klastr v systému Multiplatforms pomocí protokolu přenosu TCP/IP, postupujte takto.

z/OS V systému z/OSmusíte postupovat podle pokynů v části “Definování připojení TCP na systému z/OS” na stránce 892 , chcete-li nastavit připojení TCP/IP, spíše než definovat listenery v kroku “4” na stránce 279. Jinak jsou kroky stejné pro produkt z/OS, ale chybové zprávy se zapisují na konzolu a nikoli do protokolu chyb správce front.

Postup

1. Rozhodněte se pro organizaci klastru a jeho název.

   Rozhodli jste se propojit dva správce front, LONDON a NEWYORK, do klastru. Klastr s pouze dvěma správci front nabízí pouze okrajovou výhodu v rámci sítě, která má používat distribuované řazení do fronty. Je to dobrý způsob, jak začít, a poskytuje prostor pro budoucí expanzi. Když otevřete nové větve svého úložiště, můžete do klastru snadno přidávat nové správce front. Přidání nových správců front nenaruší existující síť; viz “Přidání správce front do klastru” na stránce 288.

   Prozatím se jedná o jedinou aplikaci, kterou spouštíte, je aplikace inventarizace. Název klastru je INVENTORY.
2. Rozhodněte se, které správci front mají uchovávat úplná úložiště.

   V každém klastru musíte navrhnout alespoň jednoho správce front, nebo nejlépe dva, aby se udržela úplná úložiště. V tomto příkladu jsou pouze dva správci front, LONDON a NEWYORK, z nichž obě zadržují úplná úložiště.

   a. Zbývající kroky můžete provést v libovolném pořadí.

   b. Při dalším postupu mohou být do protokolu správce front zapsány varovné zprávy. Zprávy jsou výsledkem chybějících definic, které jste ještě přidali.

```
Examples of the responses to the commands are shown in a box
like this after each step in this task.
These examples show the responses returned by IBM MQ for AIX.
The responses vary on other platforms.
```

c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštění správci front.

3. Upravte definice správce front tak, aby byly přidány definice úložiště.

   V každém správci front, který má uchovávat úplné úložiště, změňte definici lokálního správce front pomocí příkazu ALTER QMGR a zadáním atributu REPOS :

```
ALTER QMGR REPOS(INVENTORY)
```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: IBM MQ queue manager changed.
```

   Zadáte-li například:

   a. runmqsc LONDON

   b. ALTER QMGR REPOS(INVENTORY)

   LONDON se změní na úplné úložiště.

4. Definujte moduly listener.

   Definujte modul listener, který přijímá požadavky na síť od ostatních správců front pro každého správce front v klastru. Na správcích front produktu LONDON zadejte následující příkaz:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
```

   Atribut CONTROL zajišťuje, že se modul listener spustí a zastaví v okamžiku, kdy správce front ano.

   Listener není spuštěn, když je definován, takže musí být ručně spuštěn poprvé s následujícím příkazem MQSC:

```
START LISTENER(LONDON_LS)
```

   Vydejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každou z nich.

   Existuje několik způsobů, jak tyto listenery definovat, jak je zobrazeno v Listenerech.

5. Definujte kanál CLUSRCVR pro správce front LONDON .

   V každém správci front v klastru můžete definovat kanál příjemce klastru, v němž může správce front přijímat zprávy. Viz Channel-receiver channel: CLUSRCVR . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, na které se mohou odkazovat další správci front. Klíčové slovo CLUSTER zobrazuje dostupnost správce front pro příjem zpráv od jiných správců front v klastru.

   V tomto příkladu je název kanálu INVENTORY.LONDONa název připojení (CONNAME) je síťová adresa počítače, kde se nachází správce front, což je LONDON.CHSTORE.COM. Adresu sítě lze zadat jako alfanumerický název hostitele DNS nebo adresu IP ve tečkové desítkové tečkové notaci IPv4 . Příklad: 192.0.2.0nebo hexadecimální tvar IPv6 ; například 2001:DB8:0204:acff:fe97:2c34:fde0:3485. Číslo portu není uvedeno, takže se použije výchozí port (1414).

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
AMQ8014: WebSphere MQ channel created.
07/09/98 12:56:35 No repositories for cluster 'INVENTORY'
```

6. Definujte kanál CLUSRCVR pro správce front NEWYORK .

   Pokud modul listener kanálu používá výchozí port, obvykle 1414, a klastr neobsahuje správce front v produktu z/OS, můžete parametr CONNAME vynechat.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
```

7. Definujte kanál CLUSSDR na správci front LONDON .

   Kanál CLUSSDR můžete ručně definovat ze všech správců front úplného úložiště do všech ostatních správců front úplného úložiště v klastru. Viz Odesílací kanál klastru: CLUSSDR . V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který ukazuje na kanál CLUSRCVR definovaný v jiném správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Má-li správce front definice pro kanál příjemce klastru a odesílací kanál klastru ve stejném klastru, bude kanál odesílatele klastru spuštěn.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: WebSphere MQ channel created.
07/09/98 13:00:18  Channel program started.
```

8. Definujte kanál CLUSSDR na správci front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from NEWYORK to repository at LONDON')
```

9. Definujte frontu klastru INVENTQ

   Definujte frontu INVENTQ ve správci front NEWYORK zadáním klíčového slova CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: WebSphere MQ queue created.
```

   Klíčové slovo CLUSTER způsobí, že fronta bude inzerována do klastru. Jakmile je fronta definována, bude zpřístupněna pro ostatní správce front v klastru. Mohou do ní odesílat zprávy, aniž by bylo nutné pro ni vytvořit definici vzdálené fronty.

   Všechny definice jsou dokončené. Na všech platformách spusťte program modulu listener na každém správci front. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

Jak pokračovat dále

Nyní jste připraveni ověřit klastr.

Související úlohy

“Nastavení klastru v systému TCP/IP s použitím více přenosových front na jednoho správce front” na stránce 281
Jedná se o jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

“Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 284
Jedná se o jedno ze stromu témat popisujících různé konfigurace pro jednoduchý klastr.

Nastavení klastru v systému TCP/IP s použitím více přenosových front na jednoho správce front

Jedná se o jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

Než začnete

Přehled klastru, který se vytváří, viz “Nastavení nového klastru” na stránce 277.

Informace o této úloze

Chcete-li nastavit klastr v systému Multiplatforms pomocí protokolu přenosu TCP/IP, postupujte takto. Správci front úložiště jsou konfigurováni pro použití jiné přenosové fronty klastru k odesílání zpráv mezi sebou a ostatním správcům front v klastru. Přidáte-li do klastru správce front, který má také používat různé přenosové fronty, postupujte podle úlohy “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 290.

Postup

1. Rozhodněte se pro organizaci klastru a jeho název.

   Rozhodli jste se propojit dva správce front, `LONDON` a `NEWYORK`, do klastru. Klastr s pouze dvěma správci front nabízí pouze okrajovou výhodu v rámci sítě, která má používat distribuované řazení do fronty. Je to dobrý způsob, jak začít, a poskytuje prostor pro budoucí expanzi. Když otevřete nové větve svého úložiště, můžete do klastru snadno přidávat nové správce front. Přidání nových správců front nenaruší existující síť; viz “Přidání správce front do klastru” na stránce 288.

   Prozatím se jedná o jedinou aplikaci, kterou spouštíte, je aplikace inventarizace. Název klastru je `INVENTORY`.
2. Rozhodněte se, které správci front mají uchovávat úplná úložiště.

   V každém klastru musíte navrhnout alespoň jednoho správce front, nebo nejlépe dva, aby se udržela úplná úložiště. V tomto příkladu jsou pouze dva správci front, `LONDON` a `NEWYORK`, z nichž obě zadržují úplná úložiště.

   a. Zbývající kroky můžete provést v libovolném pořadí.

   b. Při dalším postupu mohou být do protokolu správce front zapsány varovné zprávy. Zprávy jsou výsledkem chybějících definic, které jste ještě přidali.

   ```
   Examples of the responses to the commands are shown in a box
   like this after each step in this task.
   These examples show the responses returned by IBM MQ for AIX.
   The responses vary on other platforms.
   ```

   c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštění správci front.
3. Upravte definice správce front tak, aby byly přidány definice úložiště.

   V každém správci front, který má uchovávat úplné úložiště, změňte definici lokálního správce front pomocí příkazu `ALTER QMGR` a zadáním atributu `REPOS` :

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

```
1 : ALTER QMGR REPOS(INVENTORY)
AMQ8005: IBM MQ queue manager changed.
```

Zadáte-li například:

a. `runmqsc LONDON`

b. `ALTER QMGR REPOS(INVENTORY)`

LONDON se změní na úplné úložiště.

4. Upravte definice správce front tak, aby vytvořily samostatné přenosové fronty klastru pro každý cíl.

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

U každého správce front, kterého jste přidali do klastru, se rozhodněte, zda chcete použít samostatné přenosové fronty nebo ne. Viz témata “Přidání správce front do klastru” na stránce 288 a “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 290.

5. Definujte moduly listener.

Definujte modul listener, který přijímá požadavky na síť od ostatních správců front pro každého správce front v klastru. Na správcích front produktu LONDON zadejte následující příkaz:

```
DEFINE LISTENER(LONDON_LS) TRPTYPE(TCP) CONTROL(QMGR)
```

Atribut CONTROL zajišťuje, že se modul listener spustí a zastaví v okamžiku, kdy správce front ano.

Listener není spuštěn, když je definován, takže musí být ručně spuštěn poprvé s následujícím příkazem MQSC:

```
START LISTENER(LONDON_LS)
```

Vydejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každou z nich.

Existuje několik způsobů, jak tyto listenery definovat, jak je zobrazeno v Listenerech.

6. Definujte kanál CLUSRCVR pro správce front LONDON .

V každém správci front v klastru můžete definovat kanál příjemce klastru, v němž může správce front přijímat zprávy. Viz Channel-receiver channel: CLUSRCVR . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, na které se mohou odkazovat další správci front. Klíčové slovo CLUSTER zobrazuje dostupnost správce front pro příjem zpráv od jiných správců front v klastru.

V tomto příkladu je název kanálu `INVENTORY.LONDON`a název připojení (`CONNAME`) je síťová adresa počítače, kde se nachází správce front, což je `LONDON.CHSTORE.COM`. Adresu sítě lze zadat jako alfanumerický název hostitele DNS nebo adresu IP ve tečkové desítkové tečkové notaci IPv4 . Příklad: `192.0.2.0`nebo hexadecimální tvar IPv6 ; například `2001:DB8:0204:acff:fe97:2c34:fde0:3485`. Číslo portu není uvedeno, takže se použije výchozí port (1414).

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager LONDON')
AMQ8014: WebSphere MQ channel created.
07/09/98 12:56:35 No repositories for cluster 'INVENTORY'
```

7. Definujte kanál CLUSRCVR pro správce front NEWYORK .

   Pokud modul listener kanálu používá výchozí port, obvykle 1414, a klastr neobsahuje správce front v produktu z/OS, můžete parametr CONNAME vynechat.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(TCP) CLUSTER(INVENTORY)
DESCR('TCP Cluster-receiver channel for queue manager NEWYORK')
```

8. Definujte kanál CLUSSDR na správci front LONDON .

   Kanál CLUSSDR můžete ručně definovat ze všech správců front úplného úložiště do všech ostatních správců front úplného úložiště v klastru. Viz Odesílací kanál klastru: CLUSSDR . V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který ukazuje na kanál CLUSRCVR definovaný v jiném správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Má-li správce front definice pro kanál příjemce klastru a odesílací kanál klastru ve stejném klastru, bude kanál odesílatele klastru spuštěn.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: WebSphere MQ channel created.
07/09/98 13:00:18  Channel program started.
```

9. Definujte kanál CLUSSDR na správci front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('TCP Cluster-sender channel from NEWYORK to repository at LONDON')
```

10. Definujte frontu klastru INVENTQ

    Definujte frontu INVENTQ ve správci front NEWYORK zadáním klíčového slova CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: WebSphere MQ queue created.
```

    Klíčové slovo CLUSTER způsobí, že fronta bude inzerována do klastru. Jakmile je fronta definována, bude zpřístupněna pro ostatní správce front v klastru. Mohou do ní odesílat zprávy, aniž by bylo nutné pro ni vytvořit definici vzdálené fronty.

    Všechny definice jsou dokončené. Na všech platformách spusťte program modulu listener na každém správci front. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

Jak pokračovat dále

Nyní jste připraveni ověřit klastr.

Související úlohy

“Nastavení klastru pomocí protokolu TCP/IP s jedinou přenosovou frontou na správce front” na stránce 278

Jedná se o jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

“Nastavení klastru pomocí LU 6.2 na systému z/OS” na stránce 284

Jedná se o jedno ze stromu témat popisujících různé konfigurace pro jednoduchý klastr.

Nastavení klastru pomocí LU 6.2 na systému z/OS

Jedná se o jedno ze stromu témat popisujících různé konfigurace pro jednoduchý klastr.

Než začnete

Přehled klastru, který se vytváří, viz “Nastavení nového klastru” na stránce 277.

Postup

1. Rozhodněte se pro organizaci klastru a jeho název.

   Rozhodli jste se propojit dva správce front, LONDON a NEWYORK, do klastru. Klastr s pouze dvěma správci front nabízí pouze okrajovou výhodu v rámci sítě, která má používat distribuované řazení do fronty. Je to dobrý způsob, jak začít, a poskytuje prostor pro budoucí expanzi. Když otevřete nové větve svého úložiště, můžete do klastru snadno přidávat nové správce front. Přidání nových správců front nenaruší existující síť; viz “Přidání správce front do klastru” na stránce 288.

   Prozatím se jedná o jedinou aplikaci, kterou spouštíte, je aplikace inventarizace. Název klastru je INVENTORY.
2. Rozhodněte se, které správci front mají uchovávat úplná úložiště.

   V každém klastru musíte navrhnout alespoň jednoho správce front, nebo nejlépe dva, aby se udržela úplná úložiště. V tomto příkladu jsou pouze dva správci front, LONDON a NEWYORK, z nichž obě zadržují úplná úložiště.

   a. Zbývající kroky můžete provést v libovolném pořadí.

   b. Při dalším postupu mohou být varovné zprávy zapsány do systémové konzoly produktu z/OS . Zprávy jsou výsledkem chybějících definic, které jste ještě přidali.

   c. Než budete pokračovat v těchto krocích, ujistěte se, že jsou spuštění správci front.
3. Upravte definice správce front tak, aby byly přidány definice úložiště.

   V každém správci front, který má uchovávat úplné úložiště, změňte definici lokálního správce front pomocí příkazu ALTER QMGR a zadáním atributu REPOS :

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

   ```
   1 : ALTER QMGR REPOS(INVENTORY)
   AMQ8005: IBM MQ queue manager changed.
   ```

   Zadáte-li například:

   a. `runmqsc LONDON`

   b. `ALTER QMGR REPOS(INVENTORY)`

   LONDON se změní na úplné úložiště.
4. Definujte moduly listener.

   z/OS Viz téma Inicializátor kanálu v systémech z/OS a “Příjem na LU 6.2” na stránce 895.

   Listener není spuštěn, když je definován, takže musí být ručně spuštěn poprvé s následujícím příkazem MQSC:

   ```
   START LISTENER(LONDON_LS)
   ```

   Vydejte podobné příkazy pro všechny ostatní správce front v klastru a změňte název modulu listener pro každou z nich.
5. Definujte kanál CLUSRCVR pro správce front LONDON .

V každém správci front v klastru můžete definovat kanál příjemce klastru, v němž může správce front přijímat zprávy. Viz Channel-receiver channel: CLUSRCVR . Kanál CLUSRCVR definuje název připojení správce front. Název připojení je uložen v úložištích, na které se mohou odkazovat další správci front. Klíčové slovo CLUSTER zobrazuje dostupnost správce front pro příjem zpráv od jiných správců front v klastru.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager LONDON')
```

```
1 : DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager LONDON')
AMQ8014: WebSphere MQ channel created.
07/09/98 12:56:35 No repositories for cluster 'INVENTORY'
```

6. Definujte kanál CLUSRCVR pro správce front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) TRPTYPE(LU62)
CONNAME(NEWYORK.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-receiver channel for queue manager NEWYORK')
```

7. Definujte kanál CLUSSDR na správci front LONDON .

   Kanál CLUSSDR můžete ručně definovat ze všech správců front úplného úložiště do všech ostatních správců front úplného úložiště v klastru. Viz Odesílací kanál klastru: CLUSSDR . V tomto případě existují pouze dva správci front, z nichž obě obsahují úplná úložiště. Každý z nich potřebuje ručně definovaný kanál CLUSSDR , který ukazuje na kanál CLUSRCVR definovaný v jiném správci front. Názvy kanálů zadané v definicích CLUSSDR se musí shodovat s názvy kanálů v odpovídajících definicích CLUSRCVR . Má-li správce front definice pro kanál příjemce klastru a odesílací kanál klastru ve stejném klastru, bude kanál odesílatele klastru spuštěn.

```
DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNAME(CPIC) CLUSTER(INVENTORY)
DESCR('LU62 Cluster-sender channel from LONDON to repository at NEWYORK')
```

```
1 : DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNAME(NEWYORK.LUNAME) CLUSTER(INVENTORY)
MODENAME('#INTER') TPNAME('MQSERIES')
DESCR('LU62 Cluster-sender channel from LONDON to repository at NEWYORK')
AMQ8014: WebSphere MQ channel created.
07/09/98 13:00:18  Channel program started.
```

8. Definujte kanál CLUSSDR na správci front NEWYORK .

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(LU62)
CONNAME(LONDON.LUNAME) CLUSTER(INVENTORY)
DESCR('LU62 Cluster-sender channel from NEWYORK to repository at LONDON')
```

9. Definujte frontu klastru INVENTQ

   Definujte frontu INVENTQ ve správci front NEWYORK zadáním klíčového slova CLUSTER .

```
DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
```

```
1 : DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
AMQ8006: WebSphere MQ queue created.
```

Klíčové slovo CLUSTER způsobí, že fronta bude inzerována do klastru. Jakmile je fronta definována, bude zpřístupněna pro ostatní správce front v klastru. Mohou do ní odesílat zprávy, aniž by bylo nutné pro ni vytvořit definici vzdálené fronty.

Všechny definice jsou dokončené. Na všech platformách spusťte program modulu listener na každém správci front. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

Jak pokračovat dále

Nyní jste připraveni ověřit klastr.

Související úlohy

"Nastavení klastru pomocí protokolu TCP/IP s jedinou přenosovou frontou na správce front" na stránce 278

Jedná se o jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

"Nastavení klastru v systému TCP/IP s použitím více přenosových front na jednoho správce front" na stránce 281

Jedná se o jedno ze tří témat popisujících různé konfigurace pro jednoduchý klastr.

Ověření klastru

Partnerské téma popisuje tři různé konfigurace jednoduchého klastru. 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 jedinou přenosovou frontou na správce front" na stránce 278.
- "Nastavení klastru v systému TCP/IP s použitím více přenosových front na jednoho správce front" na stránce 281.
- "Nastavení klastru pomocí LU 6.2 na systému z/OS" na stránce 284.

Přehled klastru, který byl vytvořen, naleznete v tématu "Nastavení nového klastru" na stránce 277.

Informace o této úloze

Klastr můžete ověřit jedním nebo více z těchto způsobů:

1. Spuštění administrativních příkazů pro zobrazení atributů klastru a kanálu.
2. Spusťte ukázkové programy pro odesílání a příjem zpráv ve frontě klastru.
3. Napište své vlastní programy, které odešlou zprávu požadavku do fronty klastru a odpoví zprávou s odpovědí na neklastrovaná frontu odpovědí.

Postup

Chcete-li ověřit klastr, zadejte příkaz DISPLAY **runmqsc** .

Odpovědi, které vidíte, by měly být jako reakce v krocích, které následují.

1. Ve správci front NEWYORK spusťte příkaz **DISPLAY CLUSQMGR** :

```
dis clusqmgr(*)
```

```
1 : dis clusqmgr(*)
AMQ8441: Display Cluster Queue Manager details.
CLUSQMGR(NEWYORK)       CLUSTER(INVENTORY)
CHANNEL(INVENTORY.NEWYORK)
AMQ8441: Display Cluster Queue Manager details.
CLUSQMGR(LONDON)        CLUSTER(INVENTORY)
CHANNEL(INVENTORY.LONDON)
```

2. Ve správci front NEWYORK spusťte příkaz **DISPLAY CHANNEL STATUS** :

```
dis chstatus(*)
```

```
1 : dis chstatus(*)
AMQ8417: Display Channel Status details.
CHANNEL(INVENTORY.NEWYORK)  XMITQ( )
CONNAME(192.0.2.0)      CURRENT
CHLTYPE(CLUSRCVR)       STATUS(RUNNING)
RQMNAME(LONDON)
AMQ8417: Display Channel Status details.
CHANNEL(INVENTORY.LONDON) XMITQ(SYSTEM.CLUSTER.TRANSMIT.INVENTORY.LONDON)
CONNAME(192.0.2.1)      CURRENT
CHLTYPE(CLUSSDR)       STATUS(RUNNING)
RQMNAME(LONDON)
```

Odesílání zpráv mezi dvěma správci front pomocí produktu **amqsput**.

3. V systému LONDON spusťte příkaz **amqsput INVENTQ LONDON**.

   Zadejte některé zprávy, za nimiž bude následovat prázdný řádek.

4. V systému NEWYORK spusťte příkaz **amqsget INVENTQ NEWYORK**.

   Nyní uvidíte zprávy, které jste zadali v systému LONDON. Po 15 sekundách se program ukončí.

Odesílání zpráv mezi dvěma správci front pomocí vašich vlastních programů.

V následujících krocích vloží LONDON zprávu do INVENTQ na NEWYORK a obdrží odpověď ve své frontě LONDON_reply.

5. V systému LONDON vložte zprávy do fronty klastru.
   a) Definujte lokální frontu s názvem LONDON_reply.
   b) Nastavte volby MQOPEN na hodnotu MQOO_OUTPUT.
   c) Zadejte volání MQOPEN pro otevření fronty INVENTQ.
   d) Nastavte název *ReplyToQ* v deskriptoru zpráv na LONDON_reply.
   e) Zadejte volání příkazu MQPUT pro vložení zprávy.
   f) Potvrďte zprávu.
6. V systému NEWYORK obdrží zprávu ve frontě klastru a vložte odpověď do fronty odpovědí.
   a) Nastavte volby MQOPEN na hodnotu MQOO_BROWSE.
   b) Zadejte volání MQOPEN pro otevření fronty INVENTQ.
   c) Chcete-li získat zprávu z produktu INVENTQ, zadejte volání MQGET.
   d) Načtěte název *ReplyToQ* z deskriptoru zprávy.
   e) Zadejte název *ReplyToQ* do pole ObjectName deskriptoru objektu.
   f) Nastavte volby MQOPEN na hodnotu MQOO_OUTPUT.
   g) Zadejte volání MQOPEN pro otevření LONDON_reply ve správci front LONDON.
   h) Zadejte volání příkazu MQPUT pro vložení zprávy do produktu LONDON_reply.
7. V systému LONDON obdržíte odpověď.
   a) Nastavte volby MQOPEN na hodnotu MQOO_BROWSE.
   b) Zadejte volání MQOPEN pro otevření fronty LONDON_reply.
   c) Zadejte volání produktu MQGET , abyste získali zprávu z produktu LONDON_reply.

Přidání správce front do klastru

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí jedné přenosové fronty klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY je nastaven tak, jak je popsáno v tématu "Nastavení nového klastru" na stránce 277. Obsahuje dva správce front, produkty LONDON a NEWYORK, které uchovávají úplná úložiště.
- Správce front PARIS je vlastněn primární instalací. Pokud tomu tak není, musíte spustit příkaz **setmqenv** , který nastaví prostředí příkazu pro instalaci, do které patří produkt PARIS .
- Konektivita TCP existuje mezi všemi třemi systémy a správce front je konfigurován s modulem listener TCP, který začíná pod kontrolou správce front.

Informace o této úloze

1. Nová větev úložiště řetězce je nastavována v Paříži a vy chcete přidat správce front s názvem PARIS do klastru.
2. Správce front PARIS odesílá aktualizace soupisu do aplikace běžící na systému v New Yorku vložením zpráv do fronty INVENTQ .

Chcete-li přidat správce front do klastru, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště PARIS odkazuje na první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile se nový správce front přidá do klastru, ihned se naučí také o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu propojíte PARIS se správcem front LONDON, a to čistě z geografických důvodů.

   Poznámka: Proveďte zbývající kroky v libovolném pořadí, po spuštění správce front PARIS .
2. Definujte kanál CLUSRCVR ve správci front PARIS.

   Každý správce front v klastru musí definovat kanál příjemce klastru, ve kterém může přijímat zprávy. V systému PARISdefinujte:

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager PARIS')
   ```

   Přijímací kanál klastru oznamuje dostupnost zpráv od jiných správců front v klastru INVENTORY. Nevytvářet definice v jiných správcích front pro odeslání do kanálu příjemce klastru INVENTORY.PARIS. Další definice se automaticky provedou, když je třeba. Viz Kanály klastru.
3. z/OS
   Spusťte inicializátor kanálu na serveru IBM MQ for z/OS.
4. Definujte kanál CLUSSDR ve správci front PARIS.

   Přidáte-li do klastru správce front, který není úplným úložištěm, definujte pouze jeden kanál odesílatele klastru, aby se počáteční připojení k úplnému úložišti stalo počátečními. Viz Odesílací kanál klastru: CLUSSDR .

V systému PARISvytvořte následující definici pro kanál CLCLSDR s názvem INVENTORY.LONDON ke správci front se síťovou adresou LONDON.CHSTORE.COM.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at LONDON')
```

5. Volitelné: Pokud přidáváte do klastru správce front, který byl již dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:
   a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, který přidáváte.

      Tento krok zastaví kanály klastru a poskytne lokální mezipaměti klastru čerstvou sadu pořadových čísel, která jsou zajištěná tak, aby byla ve zbývající části klastru až do konce.

      ```
      REFRESH CLUSTER(INVENTORY) REPOS(YES)
      ```

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

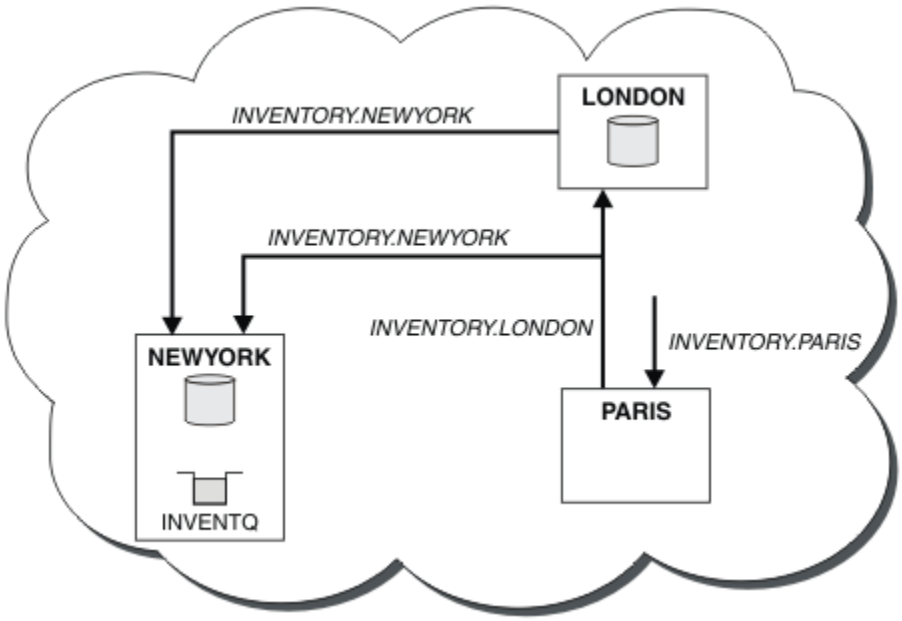
   b) Restartujte kanál CLUSSDR

      (příklad pomocí příkazu START CHANNEL).

   c) Restartujte kanál CLUSRCVR.

Výsledky

Následující obrázek ukazuje klastr, který je nastaven touto úlohou.



Obrázek 41. Klastr INVENTORY se třemi správci front

Při vytváření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR jsme přidali správce front PARIS do klastru.

Nyní se správce front produktu PARIS učí z úplného úložiště na serveru LONDON, že fronta INVENTQ je hostována správcem front NEWYORK. Když se aplikace hostovaná v systému v Paříži pokusí vložit zprávy do INVENTQ, PARIS automaticky definuje odesílací kanál klastru pro připojení k přijímacímu kanálu klastru INVENTORY.NEWYORK. Aplikace může přijímat odpovědi, je-li její název správce front zadán jako správce cílové fronty a je poskytnuta fronta pro odpověď.

Přidání správce front do klastru: samostatné přenosové fronty

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Než začnete

- Správce front není členem žádného klastru.
- Klastr existuje; existuje úplné úložiště, ke kterému se tento správce front může připojit přímo a k dispozici úložiště. Postup vytvoření klastru viz “Nastavení nového klastru” na stránce 277.

Informace o této úloze

Tato úloha je alternativou k produktu “Přidání správce front do klastru” na stránce 288, ve kterém přidáváte správce front do klastru, který umísťuje zprávy klastru do jediné přenosové fronty.

V této úloze přidáte správce front do klastru, který automaticky vytvoří oddělené přenosové fronty klastru pro každý odesílací kanál klastru.

Chcete-li zachovat malý počet definic front, použije se výchozí nastavení pro použití jediné přenosové fronty. Použití samostatných přenosových front je výhodné, chcete-li monitorovat provoz určený pro různé správce front a různé klastry. Chcete-li dosáhnout cíle izolace nebo výkonu, můžete také chtít oddělit provoz k různým místům určení.

Postup

1. Změňte výchozí typ přenosové fronty kanálu klastru.

   Změňte správce front PARIS:

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

   Pokaždé, když správce front vytvoří odesílací kanál klastru k odeslání zprávy správci front, vytvoří přenosovou frontu klastru. Přenosová fronta je používána pouze tímto odesílacím kanálem klastru. Přenosová fronta je trvalá-dynamická. Vytvoří se z modelové fronty SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUEs názvem SYSTEM.CLUSTER.TRANSMIT.*ChannelName*.

   Upozornění: Používáte-li vyhrazenou hodnotu SYSTEM.CLUSTER.TRANSMIT.QUEUES se správcem front, který byl upgradován z verze produktu starší než IBM WebSphere MQ 7.5, ujistěte se, že má SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE volbu SHARE/NOSHARE nastavenou na hodnotu **SHARE**.

2. Rozhodněte se, které úplné úložiště PARIS odkazuje na první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile se nový správce front přidá do klastru, ihned se naučí také o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu propojíte PARIS se správcem front LONDON, a to čistě z geografických důvodů.

   Poznámka: Proveďte zbývající kroky v libovolném pořadí, po spuštění správce front PARIS .

3. Definujte kanál CLUSRCVR ve správci front PARIS.

   Každý správce front v klastru musí definovat kanál příjemce klastru, ve kterém může přijímat zprávy. V systému PARISdefinujte:

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager PARIS')
   ```

Přijímací kanál klastru oznamuje dostupnost zpráv od jiných správců front v klastru INVENTORY. Nevytvářet definice v jiných správcích front pro odeslání do kanálu příjemce klastru INVENTORY.PARIS. Další definice se automaticky provedou, když je třeba. Viz Kanály klastru.

4. Definujte kanál CLUSSDR ve správci front PARIS.

   Přidáte-li do klastru správce front, který není úplným úložištěm, definujte pouze jeden kanál odesílatele klastru, aby se počáteční připojení k úplnému úložišti stalo počátečními. Viz Odesílací kanál klastru: CLUSSDR .

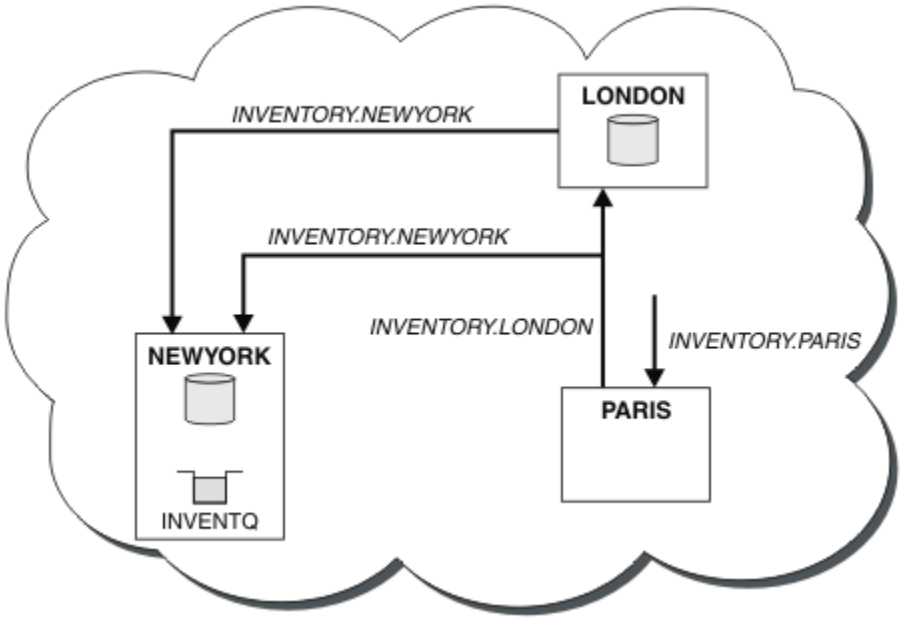
   V systému PARISvytvořte následující definici pro kanál CLCLSDR s názvem INVENTORY.LONDON ke správci front se síťovou adresou LONDON.CHSTORE.COM.

```
DEFINE CHANNEL(INVENTORY.LONDON) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
DESCR('Cluster-sender channel from PARIS to repository at LONDON')
```

   Správce front automaticky vytvoří trvalou přenosovou frontu dynamického klastru SYSTEM.CLUSTER.TRANSMIT.INVENTORY.LONDON ze modelové fronty SYSTEM.CLUSTER.TRANSMIT.MODEL.QUEUE. Nastavuje atribut CLCHNAME přenosové fronty na INVENTORY.LONDON.

Výsledky

Následující obrázek ukazuje klastr, který je nastaven touto úlohou.



Obrázek 42. Klastr INVENTORY se třemi správci front

Při vytváření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR jsme přidali správce front PARIS do klastru.

Nyní se správce front produktu PARIS učí z úplného úložiště na serveru LONDON, že fronta INVENTQ je hostována správcem front NEWYORK. Když se aplikace hostovaná v systému v Paříži pokusí vložit zprávy do INVENTQ, PARIS automaticky definuje odesílací kanál klastru pro připojení k přijímacímu kanálu klastru INVENTORY.NEWYORK. Aplikace může přijímat odpovědi, je-li její název správce front zadán jako správce cílové fronty a je poskytnuta fronta pro odpověď.

Související úlohy

Přidání správce front do klastru pomocí protokolu DHCP
Přidejte správce front do klastru pomocí protokolu DHCP. Úloha demonstruje vynechání hodnoty CONNAME v definici CLUSRCVR .

Přidání správce front do klastru pomocí protokolu DHCP

Přidejte správce front do klastru pomocí protokolu DHCP. Úloha demonstruje vynechání hodnoty CONNAME v definici CLUSRCVR .

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Úloha demonstruje dvě speciální funkce:

- Možnost vynechat hodnotu parametru CONNAME v definici CLUSRCVR .
- Schopnost používat produkt +QMNAME+ v definici CLUSSDR .

Ani jedna z funkcí není poskytována v produktu z/OS.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Nastavení nového klastru” na stránce 277. Obsahuje dva správce front, produkty LONDON a NEWYORK, které uchovávají úplná úložiště.
- Nová větev úložiště řetězce je nastavována v Paříži a vy chcete přidat správce front s názvem PARIS do klastru.
- Správce front PARIS odesílá aktualizace soupisu do aplikace běžící na systému v New Yorku vložením zpráv do fronty INVENTQ.
- Síťová konektivita existuje mezi všemi třemi systémy.
- Síťový protokol je TCP.
- Systém správce front produktu PARIS používá protokol DHCP, což znamená, že adresy IP se mohou při restartování systému změnit.
- Kanály mezi systémy PARIS a LONDON jsou pojmenovány podle definované konvence pojmenování. Konvence používá název správce front úplného úložiště v produktu LONDONsprávce front.
- Administrátoři správce front produktu PARIS nemají k dispozici žádné informace o názvu správce front v úložišti LONDON . Název správce front v úložišti LONDON se může změnit.

Informace o této úloze

Chcete-li přidat správce front do klastru pomocí protokolu DHCP, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště PARIS odkazuje na první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Vyberte jedno z úložišť jako úplné úložiště. Jakmile se nový správce front přidá do klastru, ihned se naučí také o druhém úložišti. Informace o změnách správce front se odesílají přímo do dvou úložišť. V tomto příkladu se rozhodneme propojit PARIS se správcem front LONDON, a to čistě z geografických důvodů.

   Poznámka: Proveďte zbývající kroky v libovolném pořadí, po spuštění správce front PARIS .
2. Definujte kanál CLUSRCVR ve správci front PARIS.

   Každý správce front v klastru musí definovat kanál příjemce klastru, na kterém může přijímat zprávy. V systému PARISdefinujte:

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSRCVR)
   TRPTYPE(TCP) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager PARIS')
   ```

   Přijímací kanál klastru oznamuje dostupnost zpráv od jiných správců front v klastru INVENTORY. Není třeba uvádět parametr CONNAME na přijímacím kanálu klastru. Můžete požádat IBM MQ o zjištění

jména připojení ze systému, buď vynecháním CONNAME, nebo zadáním CONNAME(' '). IBM MQ vygeneruje hodnotu CONNAME pomocí aktuální adresy IP systému; viz CONNAME . Není třeba vytvářet definice pro ostatní správce front pro odeslání na přijímacím kanálu klastru INVENTORY.PARIS. Další definice se automaticky provedou, když je třeba.

3. Definujte kanál CLUSSDR ve správci front PARIS.

   Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na který může odesílat zprávy do svého počátečního úplného úložiště. V systému PARISvytvořte následující definici pro kanál s názvem INVENTORY.+QMNAME+ ke správci front s adresou sítě LONDON.CHSTORE.COM.

   ```
   DEFINE CHANNEL(INVENTORY.+QMNAME+) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(LONDON.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at LONDON')
   ```

4. Volitelné: Pokud přidáváte do klastru správce front, který byl již dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:

   a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, který přidáváte.

      Tento krok zastaví kanály klastru a poskytne lokální mezipaměti klastru čerstvou sadu pořadových čísel, která jsou zajištěná tak, aby byla ve zbývající části klastru až do konce.

      ```
      REFRESH CLUSTER(INVENTORY) REPOS(YES)
      ```

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

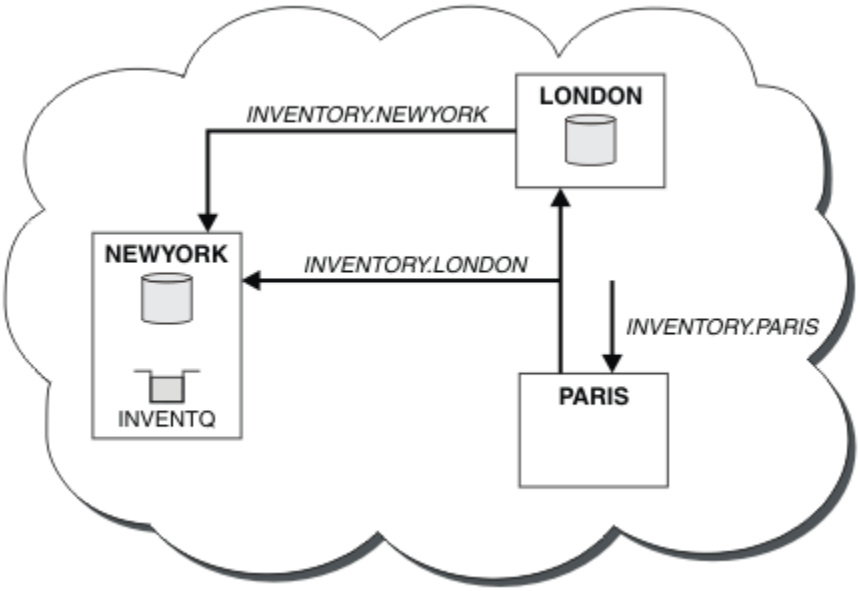
   b) Restartujte kanál CLUSSDR

      (příklad pomocí příkazu START CHANNEL).

   c) Restartujte kanál CLUSRCVR.

Výsledky

Klastr nastavený touto úlohou je stejný jako u produktu “Přidání správce front do klastru” na stránce 288:



Obrázek 43. Klastr INVENTORY se třemi správci front

Při vytváření pouze dvou definic, definice CLUSRCVR a definice CLUSSDR jsme přidali správce front PARIS do klastru.

Na správci front produktu PARIS se spustí CLUSSDR obsahující řetězec +QMNAME+ . V systému LONDON se IBM MQ interpretuje jako +QMNAME+ na název správce front (LONDON). IBM MQ se pak shoduje s definicí kanálu s názvem INVENTORY.LONDON na odpovídající definici CLUSRCVR .

Produkt IBM MQ odešle zpět vyřešený název kanálu do správce front produktu PARIS . V systému PARISje definice kanálu CLCLSDR pro kanál s názvem INVENTORY.+QMNAME+ nahrazena interně generovanou definicí CLCLSDR pro INVENTORY.LONDON. Tato definice obsahuje vyřešený název kanálu, ale jinak je stejný jako definice +QMNAME+ , kterou jste vytvořili. Úložiště klastru jsou rovněž uvedena spolu s definicí kanálu s nově vyřešeným názvem kanálu.

Poznámka:

1. Kanál vytvořený s názvem +QMNAME+ bude okamžitě neaktivní. Nikdy se nepoužívá k přenosu dat.
2. Uživatelské procedury kanálu mohou zobrazit změnu názvu kanálu mezi jedním vyvoláním a dalším vyvoláním.

Nyní se správce front produktu PARIS učí z úložiště v systému LONDON, že je hostitelem fronty INVENTQ správce front NEWYORK. Když se aplikace hostovaná v systému v Paříži pokouší vložit zprávy do INVENTQ, PARIS automaticky, definuje odesílací kanál klastru pro připojení k přijímacímu kanálu klastru INVENTORY.NEWYORK. Aplikace může přijímat odpovědi, je-li její název správce front zadán jako správce cílové fronty a je poskytnuta fronta pro odpověď.

Související úlohy

Přidání správce front do klastru: samostatné přenosové fronty

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Související odkazy

Definovat kanál

Přidání správce front, který je hostitelem fronty

Přidejte do klastru jiného správce front, aby bylo hostitelem jiné fronty produktu INVENTQ . Požadavky se odesílají střídavě do front v každém správci front. V existujícím hostiteli produktu INVENTQ není třeba provést žádné změny.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 288. Obsahuje tři správce front; LONDON a NEWYORK udržují úplná úložiště, PAŘÍŽ obsahuje dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK . Aplikace je řízena doručením zpráv ve frontě INVENTQ .
- V Torontu se vytváří nové prodejny. Chcete-li poskytnout další kapacitu, chcete-li spustit aplikaci soupisu na systému v Torontu stejně jako v New Yorku.
- Síťová konektivita existuje mezi všemi čtyřmi systémy.
- Síťový protokol je TCP.

Poznámka: Správce front TORONTO obsahuje pouze dílčí úložiště. Chcete-li do klastru přidat správce front úplného úložiště, přečtěte si téma “Přesunutí úplného úložiště do jiného správce front” na stránce 298.

Informace o této úloze

Chcete-li přidat správce front, který je hostitelem fronty, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště TORONTO odkazuje na první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. To není zvláštní význam, který úložiště si vyberete. V tomto příkladě si zvolíme NEWYORK. Poté, co se nový správce front připojil ke klastru, komunikuje s oběma úložišti.

2. Definujte kanál CLUSRCVR .

   Každý správce front v klastru musí definovat kanál příjemce klastru, na kterém může přijímat zprávy. V systému TORONTOdefinujte kanál CLUSRCVR :

   ```
   DEFINE CHANNEL(INVENTORY.TORONTO) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(TORONTO.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for TORONTO')
   ```

   Správce front produktu TORONTO inzeruje svou dostupnost přijímat zprávy od jiných správců front v klastru INVENTORY pomocí kanálu příjemce klastru.

3. Definujte kanál CLUSSDR ve správci front TORONTO.

   Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě vyberte volbu NEWYORK. Produkt TORONTO potřebuje následující definici:

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from TORONTO to repository at NEWYORK')
   ```

4. Volitelné: Pokud přidáváte do klastru správce front, který byl již dříve odebrán ze stejného klastru, zkontrolujte, zda se nyní zobrazuje jako člen klastru. Pokud ne, proveďte následující dodatečné kroky:

   a) Zadejte příkaz **REFRESH CLUSTER** ve správci front, který přidáváte.

      Tento krok zastaví kanály klastru a poskytne lokální mezipaměti klastru čerstvou sadu pořadových čísel, která jsou zajištěná tak, aby byla ve zbývající části klastru až do konce.

      ```
      REFRESH CLUSTER(INVENTORY) REPOS(YES)
      ```

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

   b) Restartujte kanál CLUSSDR

      (příklad pomocí příkazu START CHANNEL).

   c) Restartujte kanál CLUSRCVR.

5. Přezkoumejte aplikaci soupisu pro afinity zpráv.

   Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv a nainstaluje aplikaci na systém v Torontu.

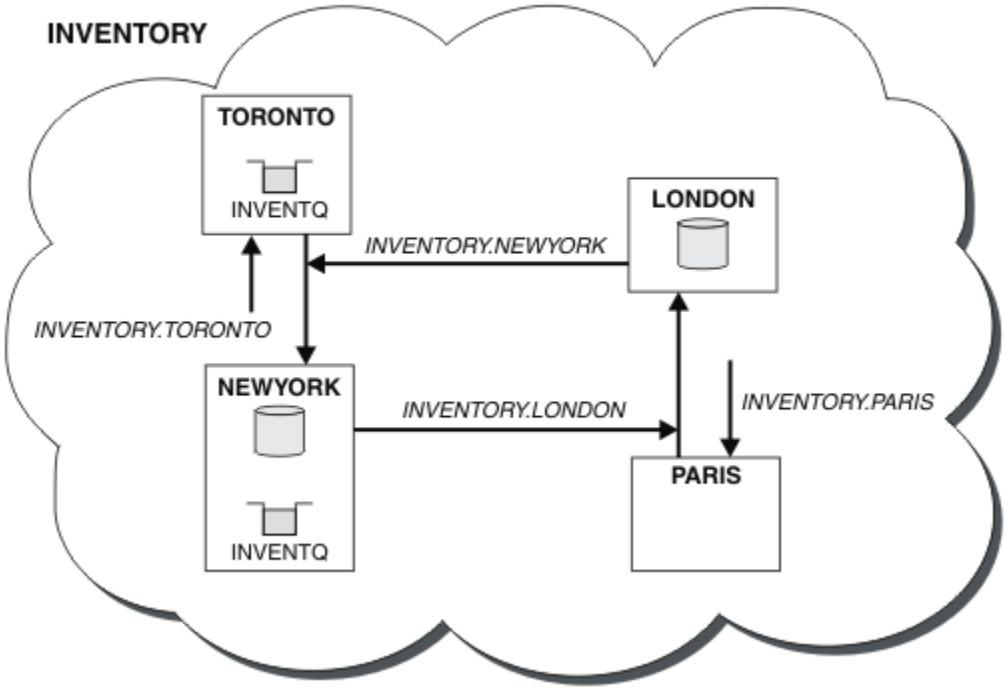
6. Definujte frontu klastru INVENTQ.

   Frontu INVENTQ , která je již hostována správcem front NEWYORK , je také hostována pomocí TORONTO. Definujte jej ve správci front produktu TORONTO takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

Výsledky

Obrázek 44 na stránce 296 zobrazuje klastr INVENTORY , který je nastaven touto úlohou.



Obrázek 44. Klastr INVENTORY se čtyřmi správci front

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správcích front v klastru. To zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje distribuci pracovní zátěže mezi dvěma správci front. Zprávy, které byly do produktu INVENTQ vloženy buď pomocí produktu TORONTO , nebo NEWYORK , jsou zpracovávány instancí v lokálním správci front, kdykoli je to možné. Zprávy ve verzi LONDON nebo PARIS jsou směrovány střídavě na TORONTO nebo NEWYORK, takže pracovní zátěž je vyvážená.

Tato úprava klastru byla dokončena, aniž byste museli měnit definice ve správcích front NEWYORK, LONDONa PARIS. Úplná úložiště v těchto správcích front jsou aktualizována automaticky s informacemi, které potřebují k odesílání zpráv do produktu INVENTQ na adrese TORONTO. Aplikace inventáře pokračuje ve funkci, pokud se jeden z NEWYORK nebo správce front TORONTO stane nedostupným a má dostatečnou kapacitu. Aplikace soupisu musí být schopna pracovat správně, je-li hostována na obou místech.

Jak můžete vidět z výsledku této úlohy, můžete mít stejnou aplikaci spuštěnou ve více než jednom správci front. Klastrování můžete rozdělit na pracovní zátěž rovnoměrně.

Aplikace nemusí být schopna zpracovat záznamy v obou lokalitách. Předpokládejme například, že jste se rozhodli přidat dotaz na zákaznický účet a aktualizovat aplikaci spuštěnou v produktu LONDON a NEWYORK. Záznam účtu může být zadržen pouze na jednom místě. Můžete se rozhodnout, že budete řídit distribuci požadavků pomocí techniky dělení dat na oblasti. Distribuci záznamů můžete rozdělit. Mohli byste uspořádat polovinu záznamů, například pro čísla účtů 00000-49999, které mají být zadrženy v LONDON. Druhá polovina, v rozsahu 50000-99999 , se nachází v NEWYORK. Pak můžete napsat uživatelský program pracovní zátěže klastru a zkontrolovat pole účtu ve všech zprávách a směrovat zprávy do příslušného správce front.

Jak pokračovat dále

Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front TORONTO. Program modulu listener čeká na příchozí síťové požadavky a spouští přijímací kanál klastru, je-li potřeba.

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 v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.
2. Skupiny sdílení front jsou podporovány pouze v systému IBM MQ for z/OS. Tato úloha se nevztahuje na jiné platformy.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Nastavení nového klastru” na stránce 277. Obsahuje dva správce front, LONDON a NEWYORK.
- Chcete přidat skupinu sdílení front do tohoto klastru. Skupina QSGPobsahuje tři správce front, P1, P2a P3. Sdílejí instanci fronty INVENTQ , která má být definována pomocí P1.

Informace o této úloze

Chcete-li přidat nové správce front, kteří jsou hostiteli sdílené fronty, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště budou správci front odkazovat jako první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť. Shromažďuje informace o klastru z úplného úložiště a skládá se tak z jeho vlastního dílčího úložiště. Není zvláštní význam toho, jaké úplné úložiště si vyberete. V tomto příkladu vyberte volbu NEWYORK. Jakmile se skupina sdílení front připojila ke klastru, komunikuje s oběma úplnými úložišti.
2. Definujte kanály CLUSRCVR .

   Každý správce front v klastru musí definovat kanál příjemce klastru, na kterém může přijímat zprávy. V systémech P1, P2a P3definujte:

   ```
   DEFINE CHANNEL(INVENTORY.Pn) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(Pn.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for sharing queue manager')
   ```

   Přijímací kanál klastru oznamuje dostupnost jednotlivých správců front přijímat zprávy od jiných správců front v klastru INVENTORY.
3. Definujte kanál CLUSSDR pro skupinu sdílení front.

   Každý člen klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK. Jeden z správců front v rámci skupiny sdílení front potřebuje následující definici skupiny. Definice zajišťuje, že každý správce front má definici kanálu odesílatele klastru.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) QSGDISP(GROUP)
   DESCR('Cluster-sender channel to repository at NEWYORK')
   ```
4. Definujte sdílenou frontu.

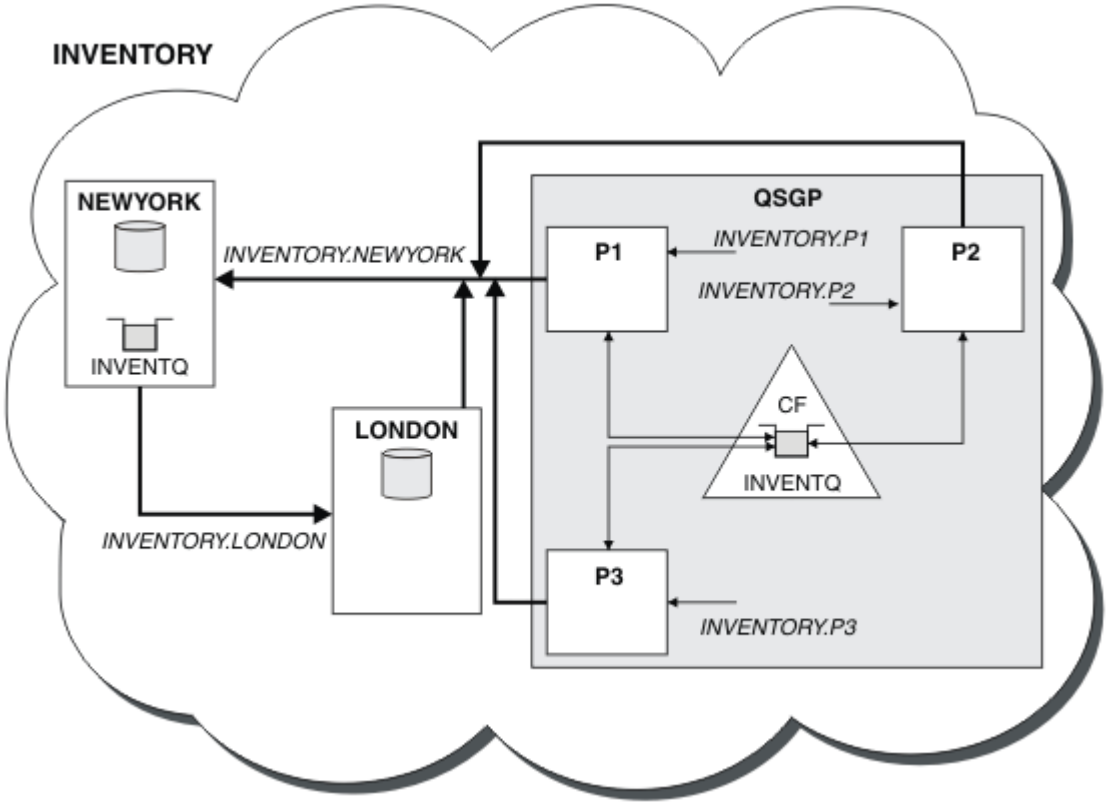
   Definujte frontu INVENTQ v systému P1 tímto způsobem:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) QSGDISP(SHARED) CFSTRUCT(STRUCTURE)
   ```

Spusťte inicializátor kanálu a program modulu listener na novém správci front. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 45 na stránce 298 zobrazuje klastr nastavený touto úlohou.



Obrázek 45. Klastr a skupina sdílení front

Nyní jsou zprávy zařazené do fronty INVENTQ produktem LONDON směrovány střídavě po čtyřech správcích front, které jsou inzerovány jako hostování fronty.

Jak pokračovat dále

Výhoda, která má členy skupiny klastrů se sdílením front, je libovolný člen skupiny může odpovědět na požadavek. V takovém případě se produkt P1 stane nedostupným po přijetí zprávy ve sdílené frontě. Místo toho může odpovědět jiný člen skupiny sdílení front.

Přesunutí úplného úložiště do jiného správce front

Přemístění úplného úložiště z jednoho správce front do jiného a sestavení nového úložiště z informací uložených ve druhém úložišti.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 288.

- Z obchodních důvodů nyní chcete odebrat úplné úložiště ze správce front LONDONa nahradit jej úplným úložištěm ve správci front PARIS. Správce front produktu NEWYORK má pokračovat v držení úplného úložiště.

Informace o této úloze

Chcete-li přesunout úplné úložiště do jiného správce front, postupujte podle následujících kroků.

Postup

1. Upravte produkt PARIS tak, aby se z něj stalo správce front úplného úložiště.

   V systému PARISzadejte následující příkaz:

   ```
   ALTER QMGR REPOS(INVENTORY)
   ```

2. Přidejte kanál CLUSSDR na PARIS

   PARIS má v současné době odesílací kanál klastru odkazující na LONDON. Produkt LONDON již nebude obsahovat úplné úložiště pro klastr. Produkt PARIS musí mít nový odesílací kanál klastru, který ukazuje na NEWYORK, kde je nyní zadrženo jiné úplné úložiště.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from PARIS to repository at NEWYORK')
   ```

3. Definujte kanál CLUSSDR na NEWYORK , který odkazuje na PARIS

   V současné době má produkt NEWYORK kanál odesílatele klastru, který ukazuje na LONDON. Nyní, když se další úplné úložiště přesunulo do produktu PARIS, je třeba přidat nový odesílací kanál klastru v NEWYORK , který ukazuje na PARIS.

   ```
   DEFINE CHANNEL(INVENTORY.PARIS) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(PARIS.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from NEWYORK to repository at PARIS')
   ```

   Když přidáte kanál odesílatele klastru do produktu PARIS, produkt PARIS se dozví o klastru z produktu NEWYORK. Staví své vlastní úplné úložiště pomocí informací z produktu NEWYORK.

4. Zkontrolujte, zda má správce front PARIS nyní úplné úložiště.

   Zkontrolujte, zda správce front PARIS vytvořil své vlastní úplné úložiště z úplného úložiště ve správci front NEWYORK. Zadejte následující příkazy:

   ```
   DIS QCLUSTER(*) CLUSTER (INVENTORY)
   DIS CLUSQMGR(*) CLUSTER (INVENTORY)
   ```

   Zkontrolujte, zda tyto příkazy zobrazují podrobnosti o stejných prostředcích v tomto klastru jako v produktu NEWYORK.

   Poznámka: Pokud správce front NEWYORK není k dispozici, nelze tuto budovu informací dokončit. Nepřesouvejte se na další krok, dokud nebude úloha dokončena.

5. Změnit definici správce front v systému LONDON

   Nakonec změňte správce front na LONDON tak, aby již nezadržuje úplné úložiště pro klastr. V systému LONDONzadejte příkaz:

   ```
   ALTER QMGR REPOS(' ')
   ```

   Správce front již nebude přijímat žádné informace o klastrech. Po 30 dnech vyprší platnost informací uložených ve svém úplném úložišti. Správce front LONDON nyní hromadí své vlastní dílčí úložiště.

6. Odeberte nebo změňte všechny neprovedené definice.

Jste-li si jisti, že nové uspořádání klastru pracuje podle očekávání, odeberte nebo změňte ručně definované definice CLUSSDR, které již nejsou správné.

- Ve správci front PARIS je třeba zastavit a odstranit kanál odesílatele klastru do produktu LONDONa poté zadat příkaz ke spuštění kanálu, aby klastr mohl znovu použít automatické kanály:

```
STOP CHANNEL(INVENTORY.LONDON)
DELETE CHANNEL(INVENTORY.LONDON)
START CHANNEL(INVENTORY.LONDON)
```

- Ve správci front NEWYORK je třeba zastavit a odstranit kanál odesílatele klastru do produktu LONDONa poté zadat příkaz ke spuštění kanálu, aby klastr mohl znovu použít automatické kanály:

```
STOP CHANNEL(INVENTORY.LONDON)
DELETE CHANNEL(INVENTORY.LONDON)
START CHANNEL(INVENTORY.LONDON)
```

- Nahraďte všechny ostatní ručně definované odesílací kanály klastru, které ukazují na LONDON ve všech správcích front v klastru, s kanály, které ukazují na NEWYORK nebo PARIS. Po odstranění kanálu vždy zadejte příkaz **start channel** , aby klastr mohl opět používat automatické kanály. V tomto malém příkladu zde nejsou žádní další. Chcete-li zkontrolovat, zda jste zapomněli, zadejte příkaz DISPLAY CHANNEL z každého správce front zadáním příkazu TYPE(CLUSSDR). Příklad:

```
DISPLAY CHANNEL(*) TYPE(CLUSSDR)
```

Je důležité, abyste tuto úlohu provedli co nejdříve po přesunu úplného úložiště z produktu LONDON do produktu PARIS. Dříve než provedete tuto úlohu, správci front, kteří mají ručně definované kanály CLUSSDR s názvem INVENTORY.LONDON , mohou odesílat požadavky na informace prostřednictvím tohoto kanálu.

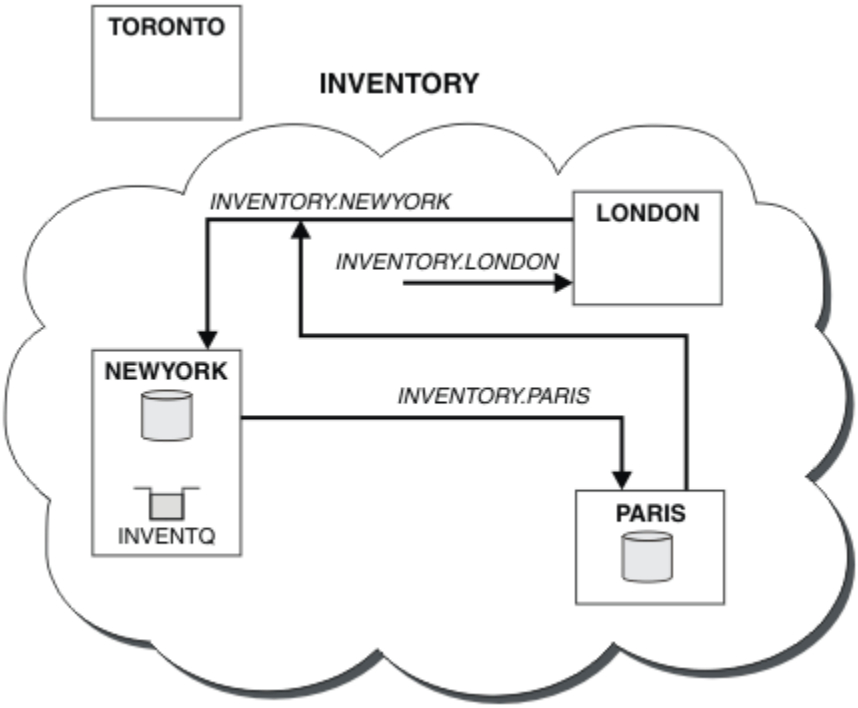
Poté, co produkt LONDON přestane být úplným úložištěm, pokud přijme takové požadavky, bude zapisovat chybové zprávy do svého protokolu chyb správce front. Následující příklady ukazují, které chybové zprávy se mohou zobrazit v produktu LONDON:

- AMQ9428: Unexpected publication of a cluster queue object received
- AMQ9432: Query received by a non-repository queue manager

Správce front LONDON neodpovídá na požadavky na informace, protože již není úplným úložištěm. Správci front, kteří požadují informace z produktu LONDON , se musí spoléhat na to, že informace o klastru budou záviset na NEWYORK , dokud nebudou ručně definované definice CLCLSDR opraveny tak, aby ukazovala na PARIS. Tato situace nesmí být tolerována jako platná konfigurace v dlouhodobém horizontu.

Výsledky

Obrázek 46 na stránce 301 zobrazuje klastr nastavený touto úlohou.



Obrázek 46. Klastr INVENTORY s úplným úložištěm byl přesunut do PARIS

Ustanovení komunikace v klastru

Inicializátor kanálu je potřebný ke spuštění komunikačního kanálu, je-li k dispozici zpráva k doručení. Modul listener kanálu čeká na spuštění druhého konce kanálu, který má přijmout zprávu.

Než začnete

Chcete-li navázat komunikaci mezi správci front v klastru, nakonfigurujte propojení pomocí jednoho z podporovaných komunikačních protokolů. Podporované protokoly jsou:

- TCP nebo LU 6.2 na libovolné platformě
- Windows Systémy NetBIOS nebo SPX v systémech Windows

Jako součást této konfigurace budete potřebovat také iniciátory kanálu a listenery kanálů stejně jako u distribuovaných front.

Informace o této úloze

Všichni správci front klastru potřebují inicializátor kanálu, aby monitoroval systémem definovanou inicializační frontu SYSTEM.CHANNEL.INITQ. SYSTEM.CHANNEL.INITQ je inicializační fronta pro všechny přenosové fronty včetně přenosové fronty klastru.

Každý správce front musí mít modul listener kanálu. Program modulu listener kanálu čeká na příchozí požadavky sítě a spustí příslušný přijímací kanál, je-li to potřeba. Implementace modulů listener kanálu je specifická pro platformu, nicméně existují některé běžné funkce.

Na všech platformách IBM MQ lze modul listener spustit pomocí příkazu **START LISTENER** .

Multi V systémech IBM i, Windows, UNIX and Linux můžete modul listener spustit automaticky ve stejnou dobu jako správce front. Chcete-li modul listener spustit automaticky, nastavte atribut CONTROL na objekt LISTENER na hodnotu QMGR nebo STARTONLY.

z/OS Nesdílený port modulu listener (INDISP (QMGR)) musí být použit pro kanály CLUSRCVR na systému z/OS a pro kanály CLUSSDR na z/OS.

Postup

1. Spusťte inicializátor kanálu.
   - z/OS V systému z/OSexistuje jeden iniciátor kanálu pro každého správce front a je spuštěn jako samostatný adresní prostor. Spustíte jej pomocí příkazu **MQSC** START CHINIT , který vydáváte jako součást spuštění správce front.
   - ULW Pokud je v produktu UNIX, Linux, and Windowsspuštěn správce front, je atribut správce front SCHINIT nastaven na hodnotu QMGR, bude inicializátor kanálu automaticky spuštěn. Jinak může být spuštěn pomocí příkazu **runmqsc** START CHINIT nebo řídicího příkazu **runmqchi** .
   - IBM i Pokud je v produktu IBM ispuštěn správce front, je atribut správce front SCHINIT nastaven na hodnotu QMGR, bude inicializátor kanálu automaticky spuštěn. Jinak může být spuštěn pomocí příkazu **runmqsc** START CHINIT nebo řídicího příkazu **runmqchi** .
2. Spusťte modul listener kanálu.
   - z/OS V systému z/OSpoužijte program modulu listener kanálu poskytovaný produktem IBM MQ. Chcete-li spustit modul listener kanálu produktu IBM MQ , použijte příkaz **MQSC** START LISTENER, který je vydáváte jako součást spuštění inicializátoru kanálu. Příklad:

     ```
     START LISTENER PORT(1414) TRPTYPE(TCP)
     ```

     nebo:

     ```
     START LISTENER LUNAME(LONDON.LUNAME) TRPTYPE(LU62)
     ```

     Členové skupiny sdílení front mohou místo modulu listener pro každého správce front používat sdílený modul listener. Nepoužívejte sdílené moduly listener s klastry. Specificky nevytvářet CONNAME objektu CLUSRCVR adresu sdíleného modulu listener skupiny sdílení front. Pokud tak učiníte, mohou správci front přijímat zprávy pro fronty, pro které nemají definici.
   - IBM i V systému IBM ipoužijte program modulu listener kanálu poskytovaný produktem IBM MQ. Chcete-li spustit modul listener kanálu produktu IBM MQ , použijte příkaz **CL** STRMQMLSR. Příklad:

     ```
     STRMQMLSR MQMNAME(QM1) PORT(1414)
     ```

   - Windows V systému Windowspoužijte buď program modulu listener kanálu poskytovaný produktem IBM MQ, nebo prostředky poskytované operačním systémem.

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

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

   - Linux UNIX V systému UNIX and Linuxpoužijte buď program modulu listener kanálu poskytovaný produktem IBM MQ, nebo prostředky poskytované operačním systémem; například **inetd** pro komunikaci TCP.

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

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

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

a. Upravte soubor `/etc/services`. Musíte být přihlášeni jako uživatel root nebo uživatel root. Pokud následující řádek není v souboru, přidejte jej podle obrázku:

```
MQSeries    1414/tcp   # WebSphere MQ channel listener
```

kde 1414 je číslo portu vyžadované produktem IBM MQ. Můžete změnit číslo portu, ale musí se shodovat s číslem portu uvedeným na konci odesílání.

b. Upravte soubor `/etc/inetd.conf`. Pokud v tomto souboru nemáte následující řádek, přidejte jej podle obrázku:

```
MQSeries stream tcp nowait mqm MQ_INSTALLATION_PATH/bin/amqcrsta amqcrsta
-m queue.manager.name
```

kde *MQ_INSTALLATION_PATH* je nahrazen vysokoúrovňovým adresářem, ve kterém je nainstalován produkt IBM MQ .

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

AIX V systému AIX:

```
refresh -s inetd
```

Solaris Linux V systémech Solaris nebo Linux:

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

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

b. Spusťte příslušný příkaz.

Pro Solaris 9 a Linux:

```
kill -1 inetd processid
```

Pro verzi produktu Solaris 10 nebo novější:

```
inetconv
```

Převod existující sítě na klastr

Převeďte existující distribuovanou síť front do klastru a přidejte dalšího správce front za účelem zvýšení kapacity.

Než začnete

V produktu “Nastavení nového klastru” na stránce 277 až “Přesunutí úplného úložiště do jiného správce front” na stránce 298 jste vytvořili a rozšířili nový klastr. Následující dva úlohy zkoumají odlišný přístup: převod existující sítě správců front na klastr.

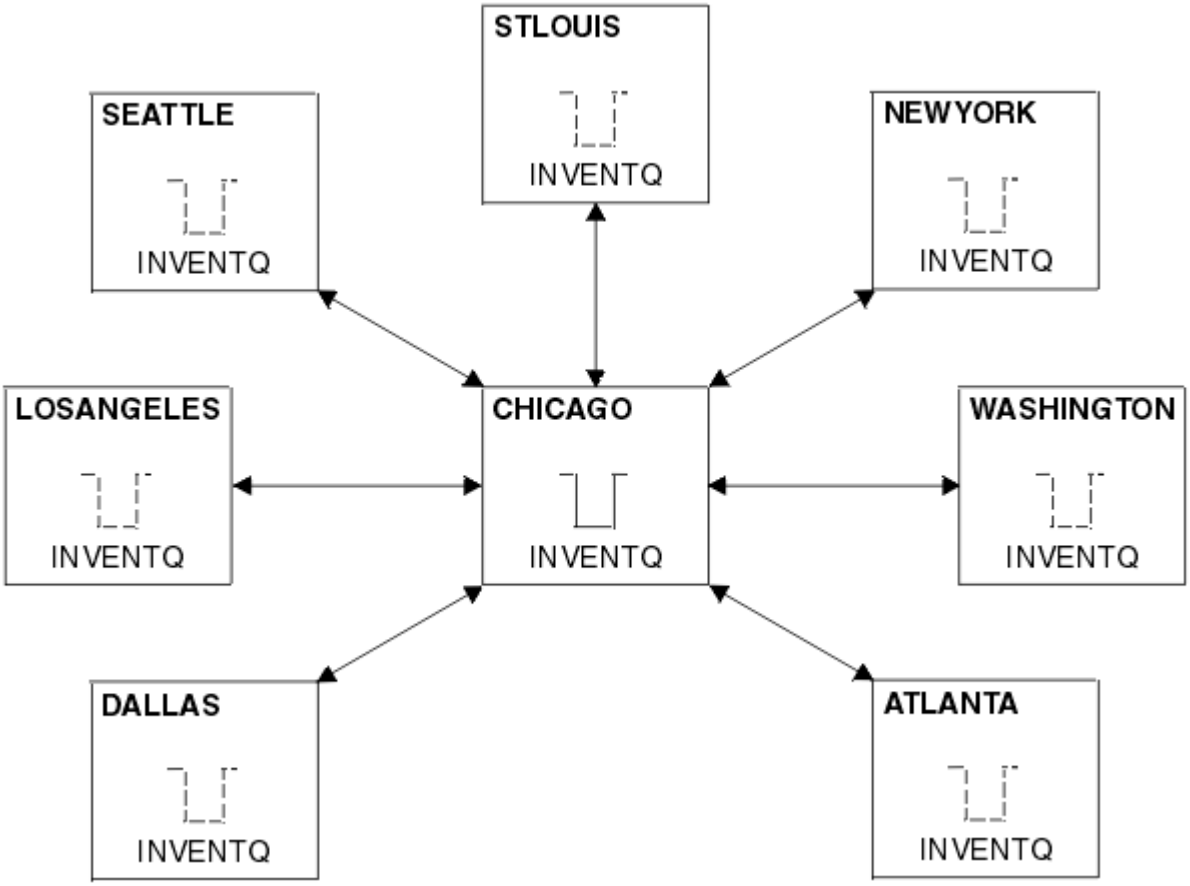
Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Síť IBM MQ je již na místě, spojující celonárodní větve řetězové databáze. Má rozbočovač a paprsek paprsek: všichni správci front jsou připojeni k jednomu správci front. Správce centrální fronty se

nachází v systému, na kterém je spuštěna aplikace zásob. Aplikace je řízena doručením zpráv ve frontě `INVENTQ` , pro které má každý správce front definici vzdálené fronty.

Tato síť je ilustrována v části Obrázek 47 na stránce 304.



Obrázek 47. Centrální a paprsek paprsek

- Chcete-li usnadnit administraci, převedete tuto síť na klastr a vytvoříte v centrálním serveru jiného správce front, který bude sdílet pracovní zátěž.

  Název klastru je `CHNSTORE`.

  Poznámka: Název klastru `CHNSTORE` byl vybrán tak, aby názvy kanálů příjemce klastru, které mají být vytvořeny, byly vytvořeny s použitím názvů ve formátu *`cluster_name. queue_manager_name`* , které nepřesahují maximální délku 20 znaků, například `CHNSTORE.WASHINGTON`.
- Oba správci front jsou hostiteli úplných úložišť a jsou přístupné pro aplikaci soupisu.
- Aplikace inventáře se má řídit přijetím zpráv ve frontě produktu `INVENTQ` , jejímž hostitelem je některý z ústředních správců front.
- Aplikace v inventáři je jedinou aplikací spuštěnou paralelně a přístupnou více než jedním správcem front. Všechny ostatní aplikace budou nadále pracovat jako dříve.
- Všechny větve mají síťovou konektivitu ke dvěma centrálním správcům front.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li převést existující síť na klastr, postupujte podle následujících kroků.

Postup

1. Přezkoumejte aplikaci soupisu pro afinity zpráv.

Než budete pokračovat, ujistěte se, že aplikace dokáže zpracovat afinity zpráv. Afinity zpráv jsou vztahy mezi dialogovými zprávami, které se vyměňují mezi dvěma aplikacemi, kde zprávy musí být zpracovány určitým správcem front nebo v určité posloupnosti. Další informace o afinitě zprávy viz: “Práce s afinitními zprávami” na stránce 379

2. Upravte dva správce centrálních front, aby z nich učinili úplné správce front úložiště.

   Dva správci front CHICAGO a CHICAGO2 jsou na centrálním serveru této sítě. Rozhodli jste se soustředit veškerou aktivitu spojenou s klastrem úložiště řetězců na tyto dva správce front. Stejně jako aplikace inventarizace a definice pro frontu INVENTQ chcete těmto správcům front hostit dvě úplná úložiště v rámci klastru. V každém ze dvou správců front zadejte následující příkaz:

   ```
   ALTER QMGR REPOS(CHNSTORE)
   ```

3. Definujte kanál CLUSRCVR pro každého správce front.

   V každém správci front v klastru definujte kanál příjemce klastru a odesílací kanál klastru. Nezáleží na tom, který kanál definujete jako první.

   Učinit definici CLUSRCVR za účelem inzerování každého správce front, jeho síťové adresy a dalších informací do klastru. Ve správci front ATLANTAnapříklad:

   ```
   DEFINE CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(ATLANTA.CHSTORE.COM) CLUSTER(CHNSTORE)
   DESCR('Cluster-receiver channel')
   ```

4. Definujte kanál CLUSSDR pro každého správce front.

   Vytvořte v každém správci front definici CLUSSDR a propojte tohoto správce front s jedním nebo více správci front úplného úložiště. Můžete například propojit ATLANTA s CHICAGO2:

   ```
   DEFINE CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(CHICAGO2.CHSTORE.COM) CLUSTER(CHNSTORE)
   DESCR('Cluster-sender channel to repository queue manager')
   ```

5. Nainstalujte aplikaci soupisu na CHICAGO2.

   You already have the inventory application on queue manager CHICAGO. Nyní je třeba vytvořit kopii této aplikace ve správci front CHICAGO2.

6. Definujte frontu INVENTQ v centrálních správcích front.

   V systému CHICAGOupravte definici lokální fronty pro frontu INVENTQ tak, aby byla fronta zpřístupněna pro klastr. Spusťte následující příkaz:

   ```
   ALTER QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
   ```

   V systému CHICAGO2vytvořte definici pro stejnou frontu:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(CHNSTORE)
   ```

   V systému z/OSmůžete použít volbu MAKEDEF funkce COMMAND produktu **CSQUTIL** k vytvoření přesné kopie produktu CHICAGO2 v produktu INVENTQ v systému CHICAGO.

   Když tyto definice provedete, odešle se zpráva do úplných úložišť na CHICAGO a CHICAGO2 a informace v nich se aktualizují. Správce front při vložení zprávy do produktu INVENTQzjistí z úplných úložišť, že pro zprávy je k dispozici volba místa určení.

7. Zkontrolujte, že změny klastru byly rozšířeny.

   Zkontrolujte, zda byly definice, které jste vytvořili v předchozím kroku, propagovány prostřednictvím klastru. Zadejte následující příkaz ve správci front úplného úložiště:

```
DIS QCLUSTER(INVENTQ)
```

Přidání nového propojeného klastru

Přidejte nový klastr, který bude sdílet některé správce front s existujícím klastrem.

Než začnete

Poznámka:

1. Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.
2. Před spuštěním této úlohy zkontrolujte kolize názvů front a porozumíte důsledkům. Možná budete muset přejmenovat frontu nebo nastavit alias fronty před tím, než budete moci pokračovat.

Scénář:

- Klastr IBM MQ byl nastaven tak, jak je popsáno v tématu “Převod existující sítě na klastr” na stránce 303.
- Je třeba implementovat nový klastr s názvem MAILORDER . Tento klastr se skládá ze čtyř správců front, kteří jsou v klastru CHNSTORE , CHICAGO, CHICAGO2, SEATTLEa ATLANTA, a dva další správce front; HARTFORD a OMAHA. Aplikace MAILORDER běží na systému v Omaha, který je připojen ke správci front OMAHA. Je řízen ostatními správci front v klastru, který vkládá zprávy do fronty produktu MORDERQ .
- Úplná úložiště pro klastr produktu MAILORDER se udržují na dvou správcích front CHICAGO a CHICAGO2.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li přidat nový propojený klastr, postupujte podle následujících kroků.

Postup

1. Vytvořte seznam názvů klastrů názvů.

   Správci front úplného úložiště na serveru CHICAGO a CHICAGO2 se nyní budou držet úplných úložišť pro oba klastry CHNSTORE a MAILORDER. Nejprve vytvořte seznam názvů obsahující názvy klastrů. Definujte seznam názvů v systémech CHICAGO a CHICAGO2následujícím způsobem:

   ```
   DEFINE NAMELIST(CHAINMAIL)
   DESCR('List of cluster names')
   NAMES(CHNSTORE, MAILORDER)
   ```

2. Upravte dvě definice správce front.

   Nyní změňte dvě definice správce front v CHICAGO a CHICAGO2. V současné době tyto definice ukazují, že správci front uchovávají úplná úložiště pro klastr CHNSTORE. Změňte tuto definici tak, aby ukazovaly, že správci front uchovávají úplná úložiště pro všechny klastry uvedené v seznamu názvů produktu CHAINMAIL . Změňte definice správce front CHICAGO a CHICAGO2 :

   ```
   ALTER QMGR REPOS(' ') REPOSNL(CHAINMAIL)
   ```

3. Upravte kanály CLUSRCVR na systémech CHICAGO a CHICAGO2.

   Definice kanálu CLUSRCVR v produktu CHICAGO a v produktu CHICAGO2 ukazují, že kanály jsou dostupné v klastru CHNSTORE. Je třeba změnit definici příjemce klastru tak, aby ukazujete, že

jsou kanály dostupné pro všechny klastry uvedené v seznamu názvů CHAINMAIL . Změňte definici přijímacího zásobníku na CHICAGO:

```
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSRCVR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

V CHICAGO2zadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSRCVR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

4. Pozměňte kanály CLUSSDR na CHICAGO a CHICAGO2.

   Změňte dvě definice kanálu CLUSSDR a přidejte seznam názvů. V CHICAGOzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

   V CHICAGO2zadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

5. Vytvořte seznam názvů v systémech SEATTLE a ATLANTA.

   Vzhledem k tomu, že SEATTLE a ATLANTA budou členy více než jednoho klastru, musíte vytvořit seznam názvů obsahující názvy klastrů. Definujte seznam názvů v systémech SEATTLE a ATLANTAnásledujícím způsobem:

```
DEFINE NAMELIST(CHAINMAIL)
DESCR('List of cluster names')
NAMES(CHNSTORE, MAILORDER)
```

6. Upravte kanály CLUSRCVR na systémech SEATTLE a ATLANTA.

   Definice kanálu CLUSRCVR v produktu SEATTLE a v produktu ATLANTA ukazují, že kanály jsou dostupné v klastru CHNSTORE. Změňte definice přijímacích kanálů klastru tak, aby ukazujete, že jsou kanály dostupné pro všechny klastry uvedené v seznamu názvů CHAINMAIL . V SEATTLEzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.SEATTLE) CHLTYPE(CLUSRCVR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

   V ATLANTAzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.ATLANTA) CHLTYPE(CLUSRCVR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

7. Pozměňte kanály CLUSSDR na SEATTLE a ATLANTA.

   Změňte dvě definice kanálu CLUSSDR a přidejte seznam názvů. V SEATTLEzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

   V ATLANTAzadejte příkaz:

```
ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR)
CLUSTER(' ') CLUSNL(CHAINMAIL)
```

8. Definujte kanály CLUSRCVR a CLUSSDR v systémech HARTFORD a OMAHA.

Ve dvou nových správcích front HARTFORD a OMAHAdefinujte příjemce klastru a odesílací kanály klastru. Nezáleží na tom, v jakém pořadí vytvoříte definice. V HARTFORDzadejte:

```
DEFINE CHANNEL(MAILORDER.HARTFORD) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(HARTFORD.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-receiver channel for HARTFORD')

DEFINE CHANNEL(MAILORDER.CHICAGO) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(CHICAGO.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-sender channel from HARTFORD to repository at CHICAGO')
```

V OMAHAzadejte:

```
DEFINE CHANNEL(MAILORDER.OMAHA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME(OMAHA.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-receiver channel for OMAHA')

DEFINE CHANNEL(MAILORDER.CHICAGO) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
CONNAME(CHICAGO.CHSTORE.COM) CLUSTER(MAILORDER)
DESCR('Cluster-sender channel from OMAHA to repository at CHICAGO')
```

9. Definujte frontu MORDERQ na OMAHA.

   Konečným krokem pro dokončení této úlohy je definovat frontu MORDERQ ve správci front OMAHA. V OMAHAzadejte:

   ```
   DEFINE QLOCAL(MORDERQ) CLUSTER(MAILORDER)
   ```

10. Zkontrolujte, že změny klastru byly rozšířeny.

    Ujistěte se, že definice, které jste vytvořili s předchozími kroky, byly rozšířeny, ačkoli klastr. Vydejte následující příkazy ve správci front úplného úložiště:

    ```
    DIS QCLUSTER (MORDERQ)
    DIS CLUSQMGR
    ```

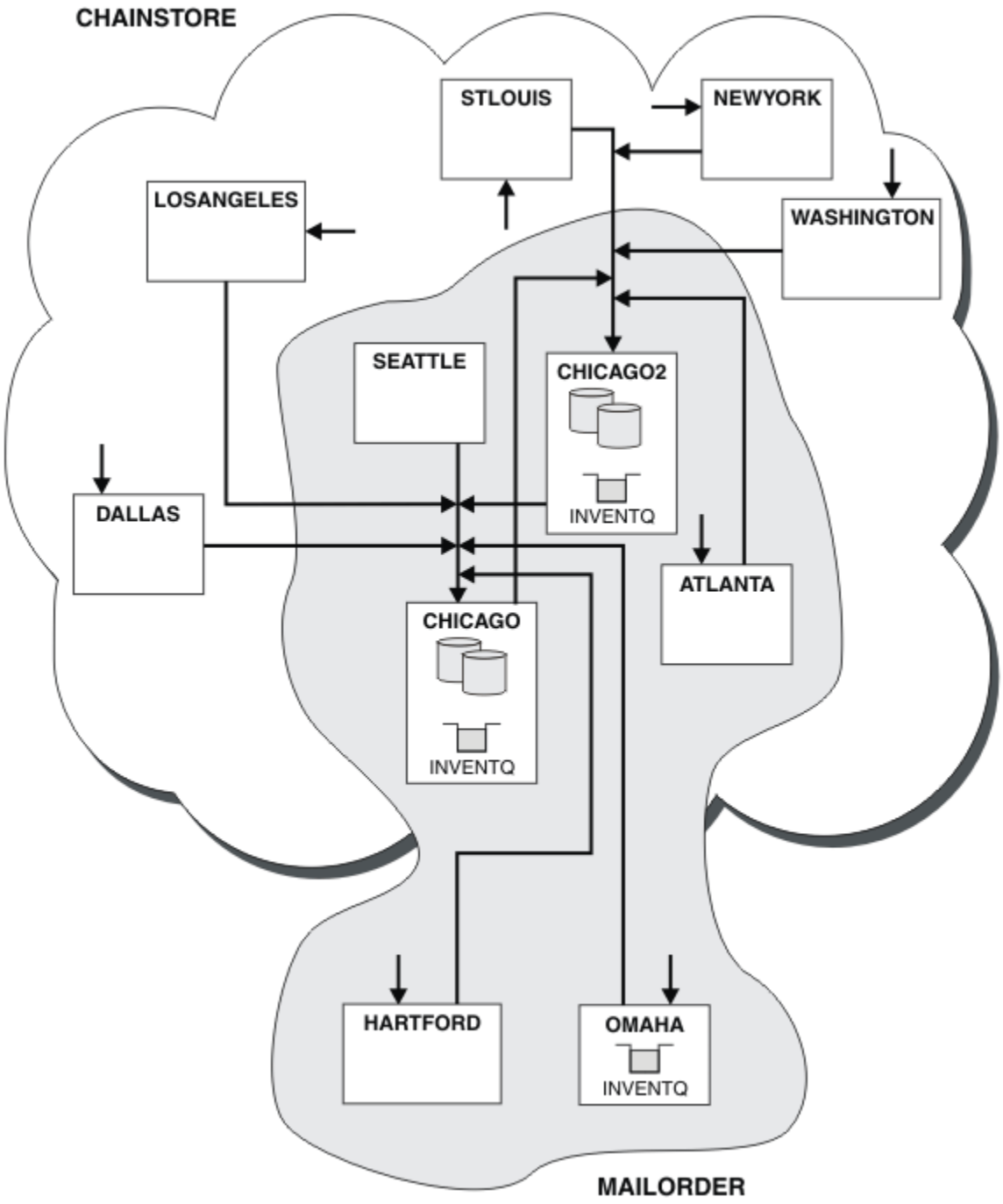
11.

Výsledky

Klastr nastavený touto úlohou se zobrazí v produktu Obrázek 48 na stránce 309.

Nyní máme dva překrývající se klastry. Úplná úložiště pro oba klastry jsou drženy v CHICAGO a CHICAGO2. Aplikace pro objednávku pošty spuštěná v produktu OMAHA je nezávislá na aplikaci soupisu, která se spouští v produktu CHICAGO. Avšak někteří správci front, kteří jsou v klastru CHNSTORE , jsou také v klastru MAILORDER , a tak mohou odesílat zprávy do jedné z aplikací. Před provedením této úlohy se překrývají dva klastry a uvědomte si, že název fronty je v rozporu.

Předpokládejme, že v systémech NEWYORK v klastru CHNSTORE a v klastru OMAHA v klastru MAILORDERexistuje fronta s názvem ACCOUNTQ. Pokud překryvy klastry a poté aplikace v produktu SEATTLE vloží zprávu do fronty ACCOUNTQ, může tato zpráva přejít buď na instanci serveru ACCOUNTQ.



Obrázek 48. Propojené klastry

Jak pokračovat dále

Předpokládejme, že se rozhodnete sloučit klastr `MAILORDER` s klastrem `CHNSTORE` a vytvořit tak jeden velký klastr s názvem `CHNSTORE`.

Chcete-li sloučit klastr `MAILORDER` s klastrem `CHNSTORE` tak, aby `CHICAGO` a `CHICAGO2` zadržovaly úplná úložiště, postupujte takto:

- Upravte definice správce front pro CHICAGO a CHICAGO2, odeberte atribut REPOSITE, který uvádí seznam názvů (CHAINMAIL), a nahraďte jej atributem REPOS, který uvádí název klastru (CHNSTORE). Například:

```
ALTER QMGR(CHICAGO) REPOSNL(' ') REPOS(CHNSTORE)
```

- U každého správce front v klastru MAILORDER změňte všechny definice kanálů a definice front tak, aby změnily hodnotu atributu CLUSTER z produktu MAILORDER na hodnotu CHNSTORE. Například v HARTFORDzadejte:

```
ALTER CHANNEL(MAILORDER.HARTFORD) CLUSTER(CHNSTORE)
```

  V OMAHA zadejte:

```
ALTER QLOCAL(MORDERQ) CLUSTER(CHNSTORE)
```

- Upravte všechny definice, které uvádějí seznam názvů klastru CHAINMAIL, tj. definice kanálu CLUSRCVR a CLUSSDR na CHICAGO, CHICAGO2, SEATTLEa ATLANTA, aby bylo možné zadat místo toho klastr CHNSTORE.

V tomto příkladu můžete vidět tu výhodu použití seznamů názvů. Místo změny definic správce front pro CHICAGO a CHICAGO2 můžete změnit hodnotu seznamu názvů CHAINMAIL. Podobně, namísto změny definic kanálů CLUSRCVR a CLUSSDR na CHICAGO, CHICAGO2, SEATTLEa ATLANTAmůžete dosáhnout požadovaného výsledku změnou seznamu názvů.

Související úlohy

Odstranění sítě klastru

Odebrat klastr ze sítě a obnovit konfiguraci distribuované fronty.

Odstranění sítě klastru

Odebrat klastr ze sítě a obnovit konfiguraci distribuované fronty.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr IBM MQ byl nastaven tak, jak je popsáno v tématu “Převod existující sítě na klastr” na stránce 303.
- Tento klastr bude nyní odebrán ze systému. Síť správců front bude nadále fungovat stejně jako předtím, než byl klastr implementován.

Informace o této úloze

Chcete-li odebrat síť klastrů, postupujte takto.

Postup

1. Odeberte fronty klastru z klastru CHNSTORE .

   V systémech CHICAGO a CHICAGO2upravte definici lokální fronty pro frontu INVENTQ tak, aby byla fronta odebrána z klastru. Spusťte následující příkaz:

```
ALTER QLOCAL(INVENTQ) CLUSTER(' ')
```

   Když změníte frontu, informace v úplných úložištích se aktualizují a šíří po celém klastru. Aktivní aplikace používající produkt MQOO_BIND_NOT_FIXEDa aplikace používající MQOO_BIND_AS_Q_DEF ,

kde byla fronta definována s DEFBIND(NOTFIXED), selžou při dalším pokusu o volání MQPUT nebo MQPUT1 . Je vrácen kód příčiny MQRC_UNKNOWN_OBJECT_NAME .

Nejprve nemusíte provést krok 1, ale pokud jej neuděláte, proveďte ji namísto po kroku 4.

2. Zastavte všechny aplikace, které mají přístup k frontě klastru.

   Zastavte všechny aplikace, které mají přístup k frontám klastru. Pokud neuděláte, mohou některé informace o klastru zůstat v lokálním správci front při aktualizaci klastru v kroku 5. Tyto informace se odeberou, když se zastaví všechny aplikace a kanály klastru se odpojí.

3. Odeberte atribut úložiště ze správců front úplného úložiště.

   V produktu CHICAGO i v produktu CHICAGO2upravte definice správce front tak, aby bylo možné odebrat atribut úložiště. Chcete-li to provést, zadejte příkaz:

   ```
   ALTER QMGR REPOS(' ')
   ```

   Správci front informují ostatní správce front v klastru o tom, že již nemají úplná úložiště. Pokud tyto informace obdrží ostatní správci front, zobrazí se zpráva označující, že bylo dokončeno úplné úložiště. Zobrazí se také jedna nebo více zpráv, které indikují, že již nejsou k dispozici žádná úložiště pro klastr CHNSTORE.

4. Odebrat kanály klastru.

   V produktu CHICAGO odeberte kanály klastru:

   ```
   ALTER CHANNEL(CHNSTORE.CHICAGO2) CHLTYPE(CLUSSDR) CLUSTER(' ')
   ALTER CHANNEL(CHNSTORE.CHICAGO) CHLTYPE(CLUSRCVR) CLUSTER(' ')
   ```

   Poznámka: Je důležité nejprve zadat příkaz CLUSSDR , poté příkaz CLUSRCVR . Nevystavujte nejprve příkaz CLUSRCVR , pak příkaz CLUSSDR . Pokud tak učiníte, vytvoříte neověřené kanály, které mají stav STOPPED . Poté je třeba vydat příkaz START CHANNEL pro zotavení zastavených kanálů; například START CHANNEL(CHNSTORE.CHICAGO).

   Zobrazí se zprávy označující, že pro klastr CHNSTOREneexistují žádná úložiště.

   Pokud jste neodebrali fronty klastru, jak je popsáno v kroku 1, udělejte to nyní.

5. Zastavit kanály klastru.

   V systému CHICAGO zastavte kanály klastru s následujícími příkazy:

   ```
   STOP CHANNEL(CHNSTORE.CHICAGO2)
   STOP CHANNEL(CHNSTORE.CHICAGO)
   ```

6. Opakujte kroky 4 a 5 pro každého správce front v klastru.
7. Zastavte kanály klastru a potom odeberte všechny definice pro kanály klastru a fronty klastru z každého správce front.
8. Volitelné: Vymažte informace o klastru uložené v mezipaměti, které má správce front.

   Přestože správci front již nejsou členy klastru, každá z nich uchovává kopii informací o klastru v mezipaměti. Chcete-li tato data odebrat, prohlédněte si úlohu “Obnova správce front do stavu před klastrem” na stránce 338.

9. Nahrazení definic vzdálených front pro produkt INVENTQ

   Aby mohla síť pokračovat ve funkci, nahraďte definici vzdálené fronty pro produkt INVENTQ v každém správci front.

10. Vytoč klastr.

    Vymažte všechny definice front nebo kanálů, které již nejsou vyžadovány.

Související úlohy

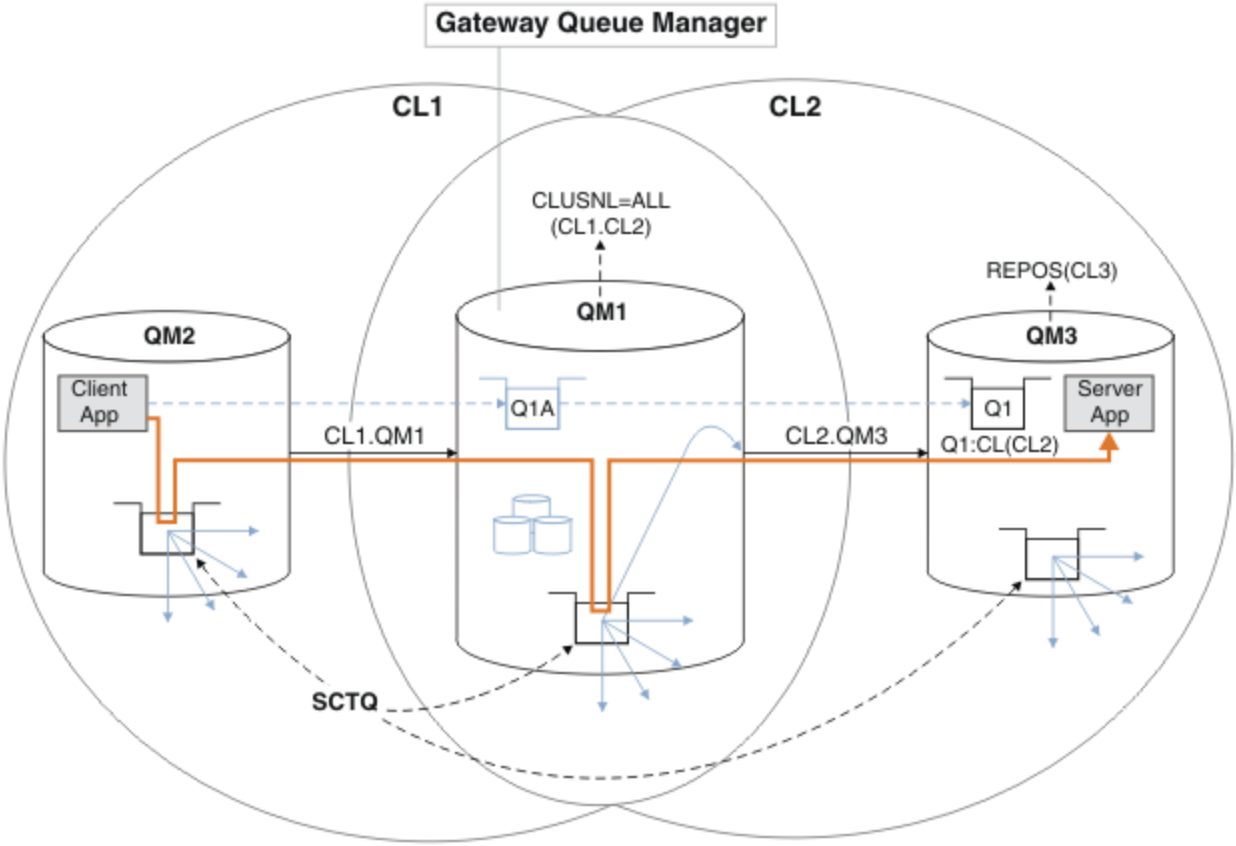
Přidání nového propojeného klastru
Přidejte nový klastr, který bude sdílet některé správce front s existujícím klastrem.

Vytvoření dvou překrývajících se klastrů se správcem front brány

Postupujte podle pokynů v úloze a vytvořte překrývající se klastry se správcem front brány. Použijte klastry jako výchozí bod pro následující příklady izolace zpráv 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 49 na stránce 312. Příklad je popsán v tématu Klastrování: Izolace aplikace pomocí více přenosových front klastru.



Obrázek 49. 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 27 na stránce 313 pro každého správce front:

Tabulka 27. 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.

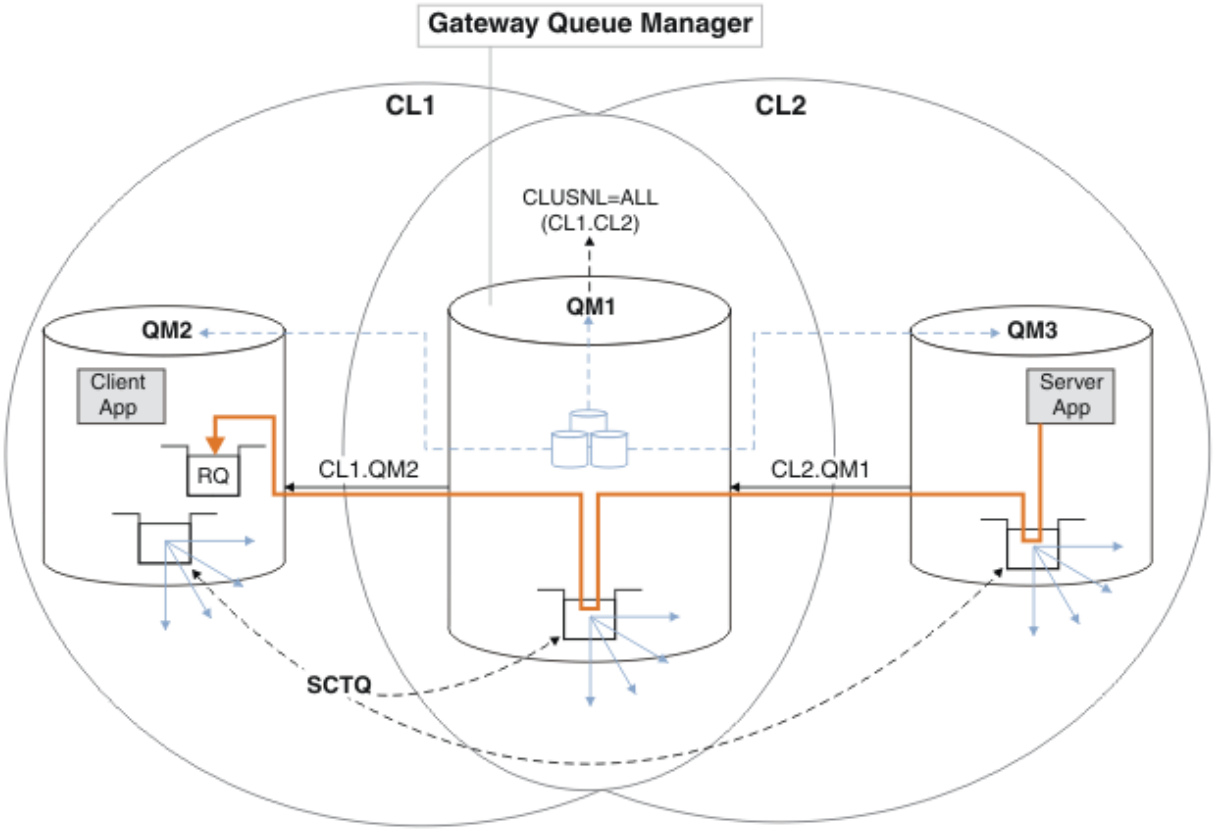
```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

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 50. 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

Související úlohy

Klastrování: Izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 290

Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

Než začnete

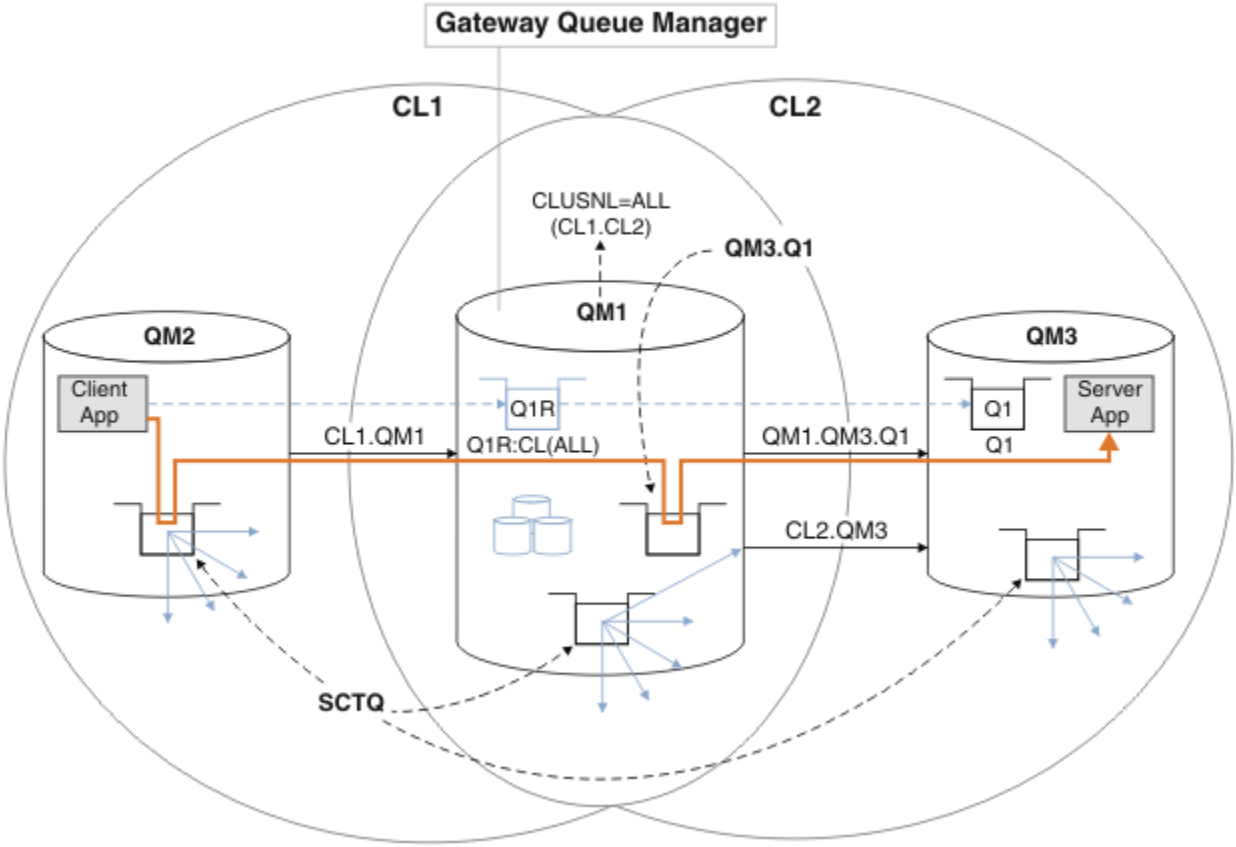
Sestavte překrývající se klastry zobrazené v aplikaci Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 312 podle kroků uvedených v této úloze.

Informace o této úloze

Řešení používá distribuované řazení do fronty k oddělení zpráv pro aplikaci `Server App` od jiných přenosů zpráv ve správci front brány. Chcete-li převést zprávy do jiné přenosové fronty a do jiného kanálu, je třeba definovat definici klastrované vzdálené fronty v produktu `QM1` . Definice vzdálené fronty musí obsahovat odkaz na konkrétní přenosovou frontu, která ukládá zprávy pouze pro produkt `Q1` v systému `QM3`. V produktu Obrázek 51 na stránce 317je alias fronty klastru `Q1A` doplněn o definici vzdálené fronty `Q1Ra` je přidána přenosová fronta a odesílací kanál.

V tomto řešení jsou všechny odpovědi vráceny pomocí obvyklých `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Výhodou tohoto řešení je to, že je snadné oddělit provoz pro více cílových front na stejném správci front, ve stejném klastru. Nevýhodou řešení je to, že nelze použít vyrovnávání pracovní zátěže klastru mezi více kopiemi produktu `Q1` v různých správcích front. Chcete-li tuto nevýhodu překonat, viz “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 319. Také musíte spravovat přepínač z jedné přenosové fronty do druhé.



Obrázek 51. Client-server aplikace implementovaná do rozbočovače a promluvila architekturu klastru pomocí definic vzdálených front

Postup

1. Vytvořit kanál pro oddělení provozu zpráv produktu `Q1` ze správce front brány
   a) Vytvořte kanál odesílatele ve správci front brány, `QM1`, do cílového správce front, `QM3`.

```
DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(SDR) CONNAME(QM3HostName(1413)) XMITQ(QM3.Q1) REPLACE
```

b) Vytvořte přijímací kanál na cílovém správci front, QM3.

```
DEFINE CHANNEL(QM1.QM3.Q1) CHLTYPE(RCVR) REPLACE
```

2. Vytvoření přenosové fronty ve správci front brány pro přenos zpráv do produktu Q1

```
DEFINE QLOCAL(QM3.Q1) USAGE(XMITQ) REPLACE
START CHANNEL(QM1.QM3.Q1)
```

Probíhá spouštění kanálu, který je přidružen k přenosové frontě, asociuje přenosovou frontu s kanálem. Kanál se spustí automaticky, jakmile je k kanálu přidružena přenosová fronta.

3. Doplňte definici aliasu klastrované fronty pro produkt Q1 ve správci front brány s definicí klastrované vzdálené fronty.

```
DEFINE QREMOTE CLUSNL(ALL) RNAME(Q1) RQMNAME(QM3) XMITQ(QM3.Q1) REPLACE
```

Jak pokračovat dále

Otestujte konfiguraci odesláním zprávy do produktu Q1 v umístění QM3 z produktu QM2 pomocí definice vzdálené fronty klastrované fronty Q1R ve správci front brány QM1.

1. Spusťte ukázkový program **amqsput** na QM2 a zadejte zprávu.

```
C:\IBM\MQ>amqsput Q1R QM2
Sample AMQSPUT0 start
target queue is Q1R
Sample request message from QM2 to Q1 using Q1R

Sample AMQSPUT0 end
```

2. Spuštěním ukázkového programu **amqsget** získáte zprávu z produktu Q1 v systému QM3 .

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1R>
no more messages
Sample AMQSGET0 end
```

Související pojmy

Řízení přístupu a více přenosových front klastru

Související úlohy

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

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

Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 290
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

Než začnete

1. Správce front brány musí být na serveru IBM WebSphere MQ 7.5nebo novějším.
2. Sestavte překrývající se klastry zobrazené v aplikaci Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 312 podle kroků uvedených v této úloze.

Informace o této úloze

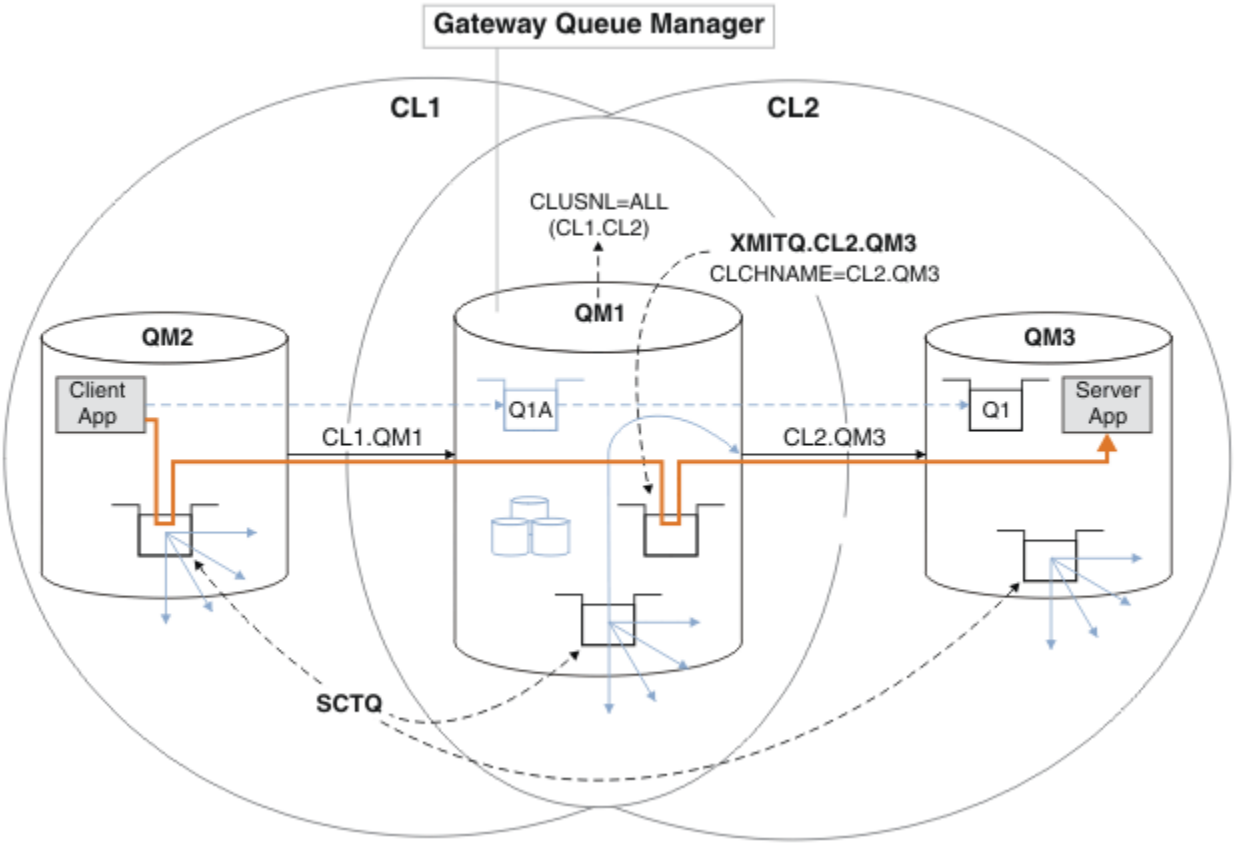
Na správci front brány, `QM1`, přidejte přenosovou frontu a nastavte její atribut fronty `CLCHNAME`. Nastavte parametr `CLCHNAME` na název přijímacího kanálu klastru v systému `QM3` . viz Obrázek 52 na stránce 320.

Toto řešení má řadu výhod oproti řešení popsanému v příručce “Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 316:

- Vyžaduje méně dodatečných definic.
- Podporuje vyvážení pracovní zátěže mezi více kopiemi cílové fronty, `Q1`, v různých správcích front ve stejném klastru, `CL2`.
- Správce front brány se automaticky přepne na novou konfiguraci, jakmile se kanál restartuje, aniž by došlo k ztrátě zpráv.
- Správce front brány pokračuje v předávání zpráv ve stejném pořadí, v jakém byla přijata. To znamená, i když se přepnutí provádí se zprávami pro frontu `Q1` v `QM3` stále na `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Konfigurace k izolování provozu zpráv klastru v produktu Obrázek 52 na stránce 320 nevedla k tomu, že by byla velká izolace provozu jako konfigurace pomocí vzdálených front v produktu “Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány” na stránce 316. Pokud správce front `QM3` v produktu `CL2` hostí řadu různých front klastru a aplikací serveru, všechny tyto fronty sdílejí kanál klastru, `CL2.QM3`, připojující se `QM1` k `QM3`. Další toky jsou ilustrovány v Obrázek 52 na stránce 320 se šedou šipkou představující potenciální provoz zpráv klastru z `SYSTEM.CLUSTER.TRANSMIT.QUEUE` do kanálu odesílatele klastru `CL2.QM3`.

Opravem je omezení správce front o hostování jedné fronty klastru v konkrétním klastru. Je-li správce front již hostitelem určitého počtu front klastru, je třeba toto omezení splnit, musíte buď vytvořit jiného správce front, nebo vytvořit jiný klastr. Viz téma “Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 322.



Obrázek 52. Client-server aplikace implementovaná do rozbočovače a promluvila o architektuře s použitím další přenosové fronty klastru.

Postup

1. Vytvořte další přenosovou frontu klastru pro odesílací kanál klastru `CL2.QM3` ve správci front brány `QM1`.

```
 *... on QM1
DEFINE QLOCAL(XMITQ.CL2.QM3) USAGE(XMITQ) CLCHNAME(CL2.QM3)
```

2. Přepněte na použití přenosové fronty `XMITQ.CL2.QM3`.
   a) Zastavte odesílací kanál klastru `CL2.QM3`.

```
*... On QM1
STOP CHANNEL(CL2.QM3)
```

   Odpověď je taková, že příkaz je přijat:

```
AMQ8019: Stop IBM MQ channel accepted.
```

   b) Zkontrolujte, zda je kanál `CL2.QM3` zastaven.

   Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou FORCE . Příklad nastavení volby FORCE by byl v případě, že se kanál nezastaví, a ostatní správce front nelze restartovat, aby se kanál synchronizoval.

```
*... On QM1
start
```

Odezva je souhrnem stavu kanálu.

```
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM3)              CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1413))      CURRENT
RQMNAME(QM3)                  STATUS(STOPPED)
SUBSTATE(MQGET)               XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

c) Spusťte kanál, `CL2.QM3`.

```
*... On QM1
START CHANNEL(CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

d) Zkontrolujte, zda je kanál spuštěn.

```
*... On QM1
DISPLAY CHSTATUS(CL2.QM3)
```

Odezva je souhrnem stavu kanálu:

```
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM3)                    CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1413))            CURRENT
RQMNAME(QM3)                        STATUS(RUNNING)
SUBSTATE(MQGET)                     XMITQ(XMITQ.CL2.QM3)
```

e) Zkontrolujte, zda byla přenosová fronta komutována.

Zkontrolujte protokol chyb správce front brány pro zprávu " AMQ7341 `Přenosová fronta pro kanál CL2.QM3 je XMITQ.CL2.QM3` ".

Jak pokračovat dále

Otestujte samostatnou přenosovou frontu odesláním zprávy z produktu `QM2` do produktu `Q1` v produktu `QM3` pomocí definice aliasu fronty `Q1A`

1. Spusťte ukázkový program **amqsput** na `QM2` , abyste vložili zprávu.

```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUT0 end
```

2. Spusťte ukázkový program **amqsget** , abyste získali zprávu z `Q1` on `QM3`

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

Související pojmy

Řízení přístupu a více přenosových front klastru

"Práce s přenosovými frontami klastru a odesílacími kanály klastru" na stránce 271
Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru. V libovolném okamžiku je kanál odesílatele klastru asociován s jednou přenosovou frontou. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizováno a transakční.

Související úlohy

Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv
Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

"Přidání správce front do klastru: samostatné přenosové fronty" na stránce 290
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

Než začnete

Kroky v úloze jsou napsány tak, aby bylo možné upravit konfiguraci ilustrované v produktu Obrázek 52 na stránce 320.

1. Správce front brány musí být na serveru IBM WebSphere MQ 7.5nebo novějším.
2. Sestavte překrývající se klastry zobrazené v aplikaci Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ v produktu "Vytvoření dvou překrývajících se klastrů se správcem front brány" na stránce 312 podle kroků uvedených v této úloze.
3. Chcete-li vytvořit řešení bez dalšího klastru, proveďte kroky uvedené v tématu Obrázek 52 na stránce 320 v produktu "Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 319 . Použijte jej jako základ pro kroky v této úloze.

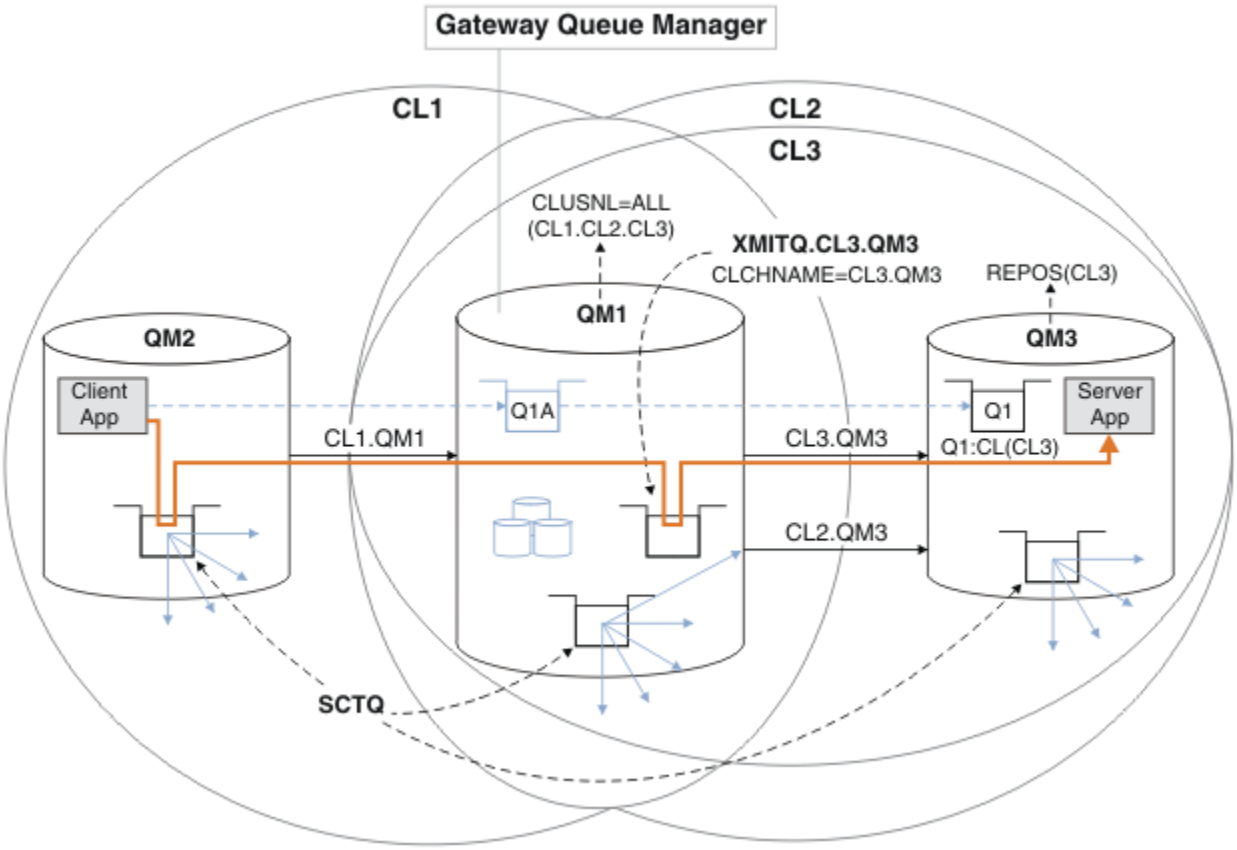
Informace o této úloze

Řešení pro izolování provozu zpráv do jediné aplikace v produktu "Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány" na stránce 319 funguje, pokud je cílová fronta klastru jedinou frontou klastru ve správci front. Pokud tomu tak není, máte dvě možnosti. Buď přesuňte frontu na jiného správce front, nebo vytvořte klastr, který izoluje danou frontu od jiných front klastru ve správci front.

Tato úloha vás provede kroky k přidání klastru k izolaci cílové fronty. Klastr je přidán pouze pro tento účel. V praxi se při navrhování klastrů a schémat pojmenování klastrů postupně přibližte k úloze izolace určitých aplikací. Přidání klastru pokaždé, když fronta vyžaduje izolaci, může skončit s mnoha klastry, které se mají spravovat. V této úloze změníte konfiguraci v produktu “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 319 přidáním klastru `CL3` za účelem izolace `Q1` v systému `QM3`. Aplikace budou pokračovat ve zpracování po celou dobu změny.

Nové a změněné definice jsou v produktu Obrázek 53 na stránce 323zvýrazněny. Souhrn změn je následující: Vytvoření klastru, což znamená, že musíte také vytvořit nové úplné úložiště klastru. V příkladu `QM3` se vytvoří jedno z úplných úložišť pro produkt `CL3`. Chcete-li přidat správce front brány do nového klastru, vytvořte odesílací kanály klastru a příjemce klastru pro produkt `QM1` . Změňte definici `Q1` tak, aby se přepnul na `CL3`. Upravte seznam názvů klastru ve správci front brány a přidejte přenosovou frontu klastru pro použití nového kanálu klastru. Nakonec přepněte alias fronty `Q1A` do nového seznamu názvů klastru.

Produkt IBM MQ nemůže přenášet zprávy z přenosové fronty `XMITQ.CL2.QM3` , které jste přidali v “Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány” na stránce 319 do nové přenosové fronty `XMITQ.CL3.QM3`, automaticky. Může přenášet zprávy automaticky pouze v případě, že obě přenosové fronty jsou obsluhovány stejným odesílacím kanálem klastru. Místo toho úloha popisuje jeden způsob, jak ručně provést přepnutí, což by mohlo být vhodné pro vás. Po dokončení přenosu máte možnost vrátit se k použití výchozí přenosové fronty klastru pro další fronty klastru `CL2` v systému `QM3`. Nebo můžete pokračovat v používání produktu `XMITQ.CL2.QM3`. Rozhodnete-li se vrátit se k výchozí přenosové frontě klastru, správce front brány pro vás automaticky spravuje přepínač.



Obrázek 53. Použití dalšího klastru k oddělení provozu zpráv ve správci front brány, který vede k jednomu z více front klastru ve stejném správci front

Postup

1. Upravte správce front QM3 a QM5 tak, aby byla úložiště pro produkty CL2 i CL3.

   Chcete-li vytvořit správce front jako člena více klastrů, je třeba použít seznam názvů klastrů k identifikaci klastrů, jejichž členem je.

   ```
   *... On QM3 and QM5
   DEFINE NAMELIST(CL23) NAMES(CL2, CL3) REPLACE
   ALTER QMGR REPOS(' ') REPOSNL(CL23)
   ```

2. Definujte kanály mezi správci front QM3 a QM5 for CL3.

   ```
   *... On QM3
   DEFINE CHANNEL(CL3.QM5) CHLTYPE(CLUSSDR) CONNAME('localhost(1415)') CLUSTER(CL3) REPLACE
   DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSRCVR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE

   *... On QM5
   DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSSDR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE
   DEFINE CHANNEL(CL3.QM5) CHLTYPE(CLUSRCVR) CONNAME('localhost(1415)') CLUSTER(CL3) REPLACE
   ```

3. Přidejte správce front brány do produktu CL3.

   Přidejte správce front brány přidáním QM1 do produktu CL3 jako dílčího úložiště. Vytvořte dílčí úložiště tak, že přidáte kanály odesílatele klastru a příjemce klastru do produktu QM1.

   Také přidejte CL3 do seznamu názvů všech klastrů připojených ke správci front brány.

   ```
   *... On QM1
   DEFINE CHANNEL(CL3.QM3) CHLTYPE(CLUSSDR) CONNAME('localhost(1413)') CLUSTER(CL3) REPLACE
   DEFINE CHANNEL(CL3.QM1) CHLTYPE(CLUSRCVR) CONNAME('localhost(1411)') CLUSTER(CL3) REPLACE
   ALTER NAMELIST(ALL) NAMES(CL1, CL2, CL3)
   ```

4. Přidejte přenosovou frontu klastru do správce front brány, QM1, pro zprávy, které se předávají produktu CL3 v systému QM3.

   Nejprve zastavte odesílací kanál klastru, který přenáší zprávy z přenosové fronty do doby, než budete připraveni přepnout přenosové fronty.

   ```
   *... On QM1
   DEFINE QLOCAL(XMITQ.CL3.QM3) USAGE(XMITQ) CLCHNAME(CL3.QM3) GET(DISABLED) REPLACE
   ```

5. Vysune zprávy z existující přenosové fronty klastru XMITQ.CL2.QM3.

   Tento dílčí postup je určen k uchování pořadí zpráv v produktu Q1 tak, aby odpovídaly pořadí, ve kterém byly obdrženy ve správci front brány. U klastrů není objednávání zpráv plně zaručeno, ale je pravděpodobné. Pokud je vyžadováno zaručené pořadí zpráv, aplikace musí definovat pořadí zpráv, viz Pořadí, v jakém se zprávy načítají z fronty.

   a) Změňte cílovou frontu Q1 na QM3 z CL2 na CL3.

      ```
      *... On QM3
      ALTER QLOCAL(Q1) CLUSTER(CL3)
      ```

   b) Monitorujte XMITQ.CL3.QM3 , dokud se do něj nezačne doručovat zprávy.

      Zprávy začínají být doručovány do XMITQ.CL3.QM3 , když je přepínač Q1 do CL3 šířen do správce front brány.

      ```
      *... On QM1
      DISPLAY QUEUE(XMITQ.CL3.QM3) CURDEPTH
      ```

   c) Monitorujte XMITQ.CL2.QM3 , dokud nebude obsahovat žádné zprávy čekající na doručení do Q1 na QM3.

      Poznámka: Produkt XMITQ.CL2.QM3 může uchovávat zprávy pro jiné fronty v produktu QM3 , které jsou členy produktu CL2. V takovém případě by hloubka nemusela přejít na nulu.

```
*... On QM1
DISPLAY QUEUE(XMITQ.CL2.QM3) CURDEPTH
```

d) Povolit získání z nové přenosové fronty klastru, XMITQ.CL3.QM3

```
*... On QM1
ALTER QLOCAL(XMITQ.CL3.QM3) GET(ENABLED)
```

6. Odstraňte starou přenosovou frontu klastru, XMITQ.CL2.QM3, pokud již není požadována.

   Zprávy pro fronty klastru v produktu CL2 v systému QM3 se vrátí k použití výchozí přenosové fronty klastru ve správci front brány QM1. Výchozí přenosová fronta klastru je buď SYSTEM.CLUSTER.TRANSMIT.QUEUE, nebo SYSTEM.CLUSTER.TRANSMIT.CL2.QM3. Který závisí na tom, zda je hodnota atributu správce front **DEFCLXQ** v systému QM1 SCTQ nebo CHANNEL. Správce front přenese zprávy z produktu XMITQ.CL2.QM3 automaticky, jakmile se spustí odesílací kanál klastru CL2.QM3 .

   a) Změňte přenosovou frontu XMITQ.CL2.QM3, aby byla přenosovou frontou klastru, aby byla normální přenosovou frontou.

      Tím dojde k přerušení přidružení přenosové fronty k libovolným odesílacím kanálům klastru. V odpovědi IBM MQ automaticky přenáší zprávy z XMITQ.CL2.QM3 do výchozí přenosové fronty klastru, když je spuštěn kanál odesílatele klastru. Do té doby jsou zprávy pro CL2 v systému QM3 stále umístěny na XMITQ.CL2.QM3.

      ```
      *... On QM1
      ALTER QLOCAL(XMITQ.CL2.QM3) CLCHNAME(' ')
      ```

   b) Zastavte odesílací kanál klastru CL2.QM3.

      Zastavení a restartování kanálu odesílatele klastru iniciuje přenos zpráv z produktu XMITQ.CL2.QM3 do výchozí přenosové fronty klastru. Zpravidla byste zastavili a spustili kanál ručně, abyste spustili přenos. Přenos se spustí automaticky, pokud se kanál restartuje po vypršení jeho intervalu odpojení.

      ```
      *... On QM1
      STOP CHANNEL(CL2.QM3)
      ```

      Odpověď je taková, že příkaz je přijat:

      ```
      AMQ8019: Stop IBM MQ channel accepted.
      ```

   c) Zkontrolujte, zda je kanál CL2.QM3 zastaven.

      Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou FORCE . Příklad nastavení volby FORCE by byl v případě, že se kanál nezastaví, a ostatní správce front nelze restartovat, aby se kanál synchronizoval.

      ```
      *... On QM1
      DISPLAY CHSTATUS(CL2.QM3)
      ```

      Odezva je souhrnem stavu kanálu.

      ```
      AMQ8417: Display Channel Status details.
      CHANNEL(CL2.QM3)                        CHLTYPE(CLUSSDR)
      CONNAME(127.0.0.1(1413))                CURRENT
      RQMNAME(QM3)                            STATUS(STOPPED)
      SUBSTATE(MQGET)                         XMITQ(XMITQ.CL2.QM3)
      ```

   d) Spusťte kanál, CL2.QM3.

```
*... On QM1
START CHANNEL(CL2.QM3)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

e) Zkontrolujte, zda je kanál spuštěn.

```
*... On QM1
DISPLAY CHSTATUS(CL2.QM3)
```

Odezva je souhrnem stavu kanálu:

```
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM3)      CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1413))  CURRENT
RQMNAME(QM3)        STATUS(RUNNING)
SUBSTATE(MQGET)      XMITQ(SYSTEM.CLUSTER.TRANSMIT. QUEUE|CL2.QM3)
```

f) Zkontrolujte protokol chyb správce front brány pro zprávu " AMQ7341 Přenosová fronta pro kanál CL2.QM3 je SYSTEM.CLUSTER.TRANSMIT. *QUEUE*|*CL2.QM3* ".

g) Odstraňte přenosovou frontu klastru, XMITQ.CL2.QM3.

```
*... On QM1
DELETE QLOCAL(XMITQ.CL2.QM3)
```

Jak pokračovat dále

Otestujte odděleně klastrovanou frontu odesláním zprávy z produktu QM2 do produktu Q1 v produktu QM3 s použitím definice aliasu fronty Q1A

1. Spusťte ukázkový program **amqsput** na QM2 , abyste vložili zprávu.

```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUT0 end
```

2. Spusťte ukázkový program **amqsget** , abyste získali zprávu z Q1 on QM3

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

Související pojmy

Řízení přístupu a více přenosových front klastru

“Práce s přenosovými frontami klastru a odesílacími kanály klastru” na stránce 271

Zprávy mezi správci front s klastry se ukládají do přenosových front klastru a předávají je kanály odesílatele klastru. V libovolném okamžiku je kanál odesílatele klastru asociován s jednou přenosovou frontou. Změníte-li konfiguraci kanálu, může se při příštím spuštění přepnout do jiné přenosové fronty. Zpracování tohoto přepínače je automatizováno a transakční.

Související úlohy

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

Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

Změna výchozí hodnoty pro oddělené přenosové fronty klastru k izolaci provozu zpráv
Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 290
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

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

Výchozí způsob, jakým správce front ukládá zprávy pro klastrovanou frontu nebo téma v přenosové frontě, můžete změnit. Změna výchozí hodnoty vám poskytuje způsob, jak izolovat zprávy klastru ve správci front brány.

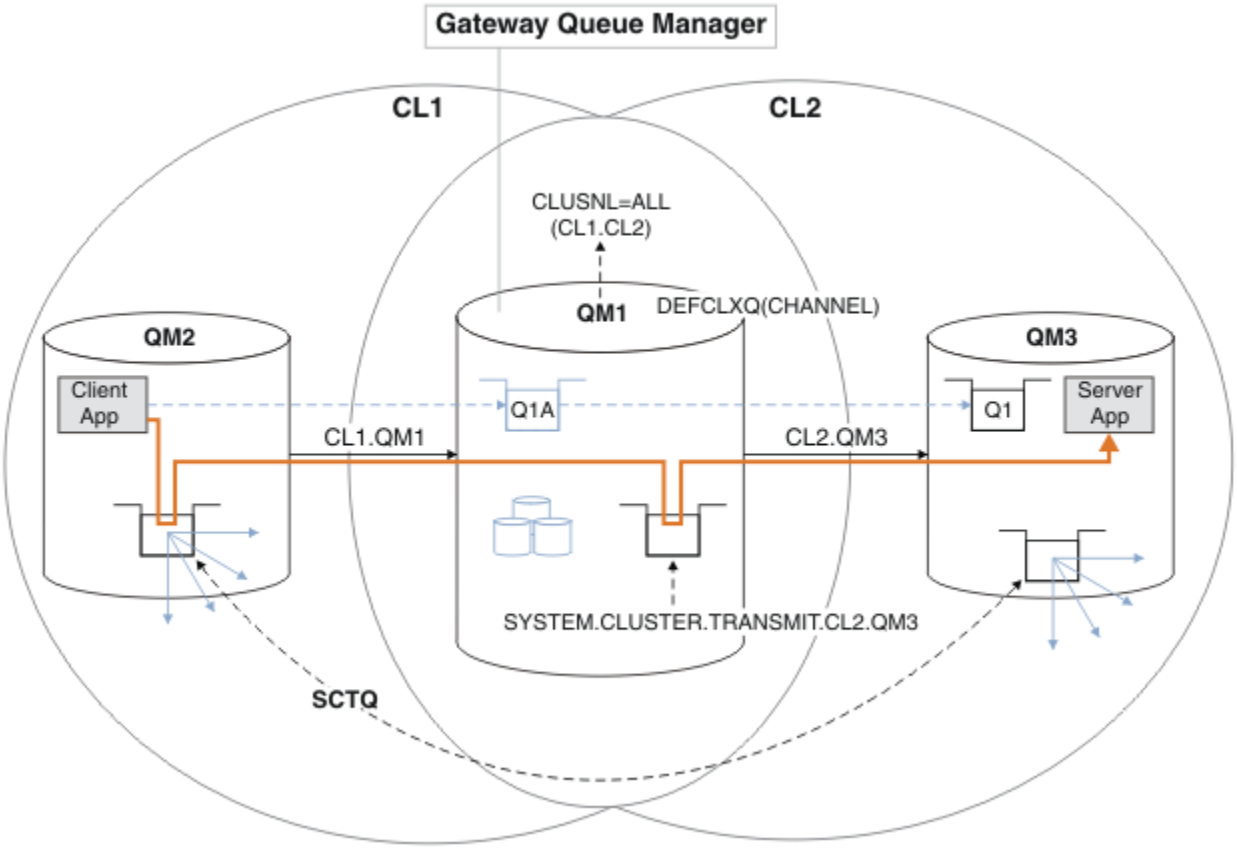
Než začnete

1. Správce front brány musí být na serveru IBM WebSphere MQ 7.5nebo novějším.
2. Sestavte překrývající se klastry zobrazené v aplikaci Client-server aplikace implementované do rozbočovače a spodanou architekturou pomocí klastrů produktu IBM MQ v produktu “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 312 podle kroků uvedených v této úloze.

Informace o této úloze

Chcete-li implementovat architekturu s více frontami klastru, musí být správce front brány na serveru IBM WebSphere MQ 7.5nebo novějším. Chcete-li pro správce front brány změnit výchozí typ přenosové fronty klastru, je třeba změnit výchozí typ přenosové fronty klastru. Změňte hodnotu atributu správce front **DEFCLXQ** na `QM1` z `SCTQ` na `CHANNEL` ; viz Obrázek 54 na stránce 328. Diagram zobrazuje jeden tok zpráv. Pro toky do jiných správců front nebo do jiných klastrů správce front vytvoří další trvalé přenosové fronty dynamického dynamického klastru. Každý odesílací kanál klastru přenáší zprávy z jiné přenosové fronty klastru.

Změna se neprojeví okamžitě, pokud nechcete poprvé připojit správce front brány k klastrům. Úloha zahrnuje kroky pro typický případ správy změny na existující konfiguraci. Chcete-li nastavit správce front tak, aby při prvním připojení ke klastru používal oddělené přenosové fronty klastru, přečtěte si téma “Přidání správce front do klastru: samostatné přenosové fronty” na stránce 290.



Obrázek 54. Client-server aplikace implementovaná do rozbočovače a spoke architektury s oddělenými frontami přenosu klastru ve správci front brány.

Postup

1. Změňte správce front brány tak, aby používal oddělené přenosové fronty klastru.

```
*... On QM1
ALTER QMGR DEFCLXQ(CHANNEL)
```

2. Přepněte na samostatné přenosové fronty klastru.

   Libovolný odesílací kanál klastru, který při příštím spuštění nespouští přepínače při použití oddělených přenosových front klastru.

   Chcete-li přepnout spuštěné kanály, buď znovu spusťte správce front, nebo postupujte takto:

   a) Seznam odesílacích kanálů klastru, které jsou spuštěny s produktem SYSTEM.CLUSTER.TRANSMIT.QUEUE.

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
```

   Odezva je seznam sestav stavu kanálu:

```
AMQ8417: Display Channel Status details.
CHANNEL(CL1.QM2)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1412))    CURRENT
RQMNAME(QM2)                STATUS(RUNNING)
SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
```

```
CHANNEL(CL2.QM3)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1413))    CURRENT
RQMNAME(QM3)                STATUS(RUNNING)
SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM5)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1415))    CURRENT
RQMNAME(QM5)                STATUS(RUNNING)
SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL(CL1.QM4)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1414))    CURRENT
RQMNAME(QM4)                STATUS(RUNNING)
SUBSTATE(MQGET)             XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

b) Zastavit spuštěné kanály

Pro každý kanál v seznamu spusťte příkaz:

```
*... On QM1
STOP CHANNEL(ChannelName)
```

Kde *ChannelName* je každý z `CL1.QM2, CL1.QM4, CL1.QM3, CL1.QM5`.

Odpověď je taková, že příkaz je přijat:

```
AMQ8019: Stop IBM MQ channel accepted.
```

c) Monitorovat, které kanály jsou zastavené

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
```

Odezva je seznam kanálů, které jsou stále spuštěné, a kanály, které jsou zastaveny:

```
AMQ8417: Display Channel Status details.
CHANNEL(CL1.QM2)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1412))    CURRENT
RQMNAME(QM2)                STATUS(STOPPED)
SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM3)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1413))    CURRENT
RQMNAME(QM3)                STATUS(STOPPED)
SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM5)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1415))    CURRENT
RQMNAME(QM5)                STATUS(STOPPED)
SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
AMQ8417: Display Channel Status details.
CHANNEL(CL1.QM4)            CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1414))    CURRENT
RQMNAME(QM4)                STATUS(STOPPED)
SUBSTATE( )                 XMITQ(SYSTEM.CLUSTER.TRANSMIT.QUEUE)
```

d) Spusťte každý zastavený kanál.

Tento krok proveďte pro všechny spuštěné kanály. Pokud se kanál nezastaví, můžete znovu spustit příkaz **STOP CHANNEL** s volbou FORCE . Příklad nastavení volby FORCE by byl v případě, že se kanál nezastaví, a ostatní správce front nelze restartovat, aby se kanál synchronizoval.

```
*... On QM1
START CHANNEL(CL2.QM5)
```

Odpověď je taková, že příkaz je přijat:

```
AMQ8018: Start IBM MQ channel accepted.
```

e) Monitorujte komutované přenosové fronty.

Zkontrolujte protokol chyb správce front brány pro zprávu " AMQ7341 Přenosová fronta pro kanál CL2.QM3 je SYSTEM.CLUSTER.TRANSMIT. *QUEUE*|*CL2.QM3* ".

f) Zkontrolujte, zda již SYSTEM.CLUSTER.TRANSMIT.QUEUE není používáno.

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ EQ 'SYSTEM.CLUSTER.TRANSMIT.QUEUE')
DISPLAY QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE) CURDEPTH
```

Odezva je seznam stavových zpráv kanálu a hloubka produktu SYSTEM.CLUSTER.TRANSMIT.QUEUE:

```
AMQ8420: Channel Status not found.
AMQ8409: Display Queue details.
QUEUE(SYSTEM.CLUSTER.TRANSMIT.QUEUE)    TYPE(QLOCAL)
CURDEPTH(0)
```

g) Monitorovat, které kanály jsou spuštěny

```
*... On QM1
DISPLAY CHSTATUS(*) WHERE(XMITQ LK 'SYSTEM.CLUSTER.TRANSMIT.*')
```

Odezva je seznam kanálů, v tomto případě již je spuštěn s novými výchozími přenosovými frontami klastru:

```
AMQ8417: Display Channel Status details.
CHANNEL(CL1.QM2)                        CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1412))                CURRENT
RQMNAME(QM2)                            STATUS(RUNNING)
SUBSTATE(MQGET)
XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL1.QM2)
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM3)                        CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1413))                CURRENT
RQMNAME(QM3)                            STATUS(RUNNING)
SUBSTATE(MQGET)
XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL2.QM3)
AMQ8417: Display Channel Status details.
CHANNEL(CL2.QM5)                        CHLTYPE(CLUSSDR)
CONNAME(127.0.0.1(1415))                CURRENT
RQMNAME(QM5)                            STATUS(RUNNING)
SUBSTATE(MQGET)
XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL2.QM5)
AMQ8417: Display Channel Status details.
CHANNEL(CL1.QM4)                        CHLTYPE(CLUSSDR)
```

```
CONNAME(127.0.0.1(1414))                CURRENT
RQMNAME(QM4)                            STATUS(RUNNING)
SUBSTATE(MQGET)
XMITQ(SYSTEM.CLUSTER.TRANSMIT.CL1.QM4)
```

Jak pokračovat dále

1. Testujte automaticky definovanou přenosovou frontu klastru odesláním zprávy z produktu QM2 do produktu Q1 v systému QM3a s definicí názvu fronty s definicí aliasu fronty Q1A .
   a. Spusťte ukázkový program **amqsput** na QM2 , abyste vložili zprávu.

```
C:\IBM\MQ>amqsput Q1A QM2
Sample AMQSPUT0 start
target queue is Q1A
Sample request message from QM2 to Q1 using Q1A

Sample AMQSPUT0 end
```

   b. Spusťte ukázkový program **amqsget** , abyste získali zprávu z Q1 on QM3

```
C:\IBM\MQ>amqsget Q1 QM3
Sample AMQSGET0 start
message <Sample request message from QM2 to Q1 using Q1A>
no more messages
Sample AMQSGET0 end
```

2. Zvažte, zda znovu konfigurovat zabezpečení, a to konfigurací zabezpečení pro fronty klastru na správci front, odkud pocházejí zprávy pro fronty klastru.

Související pojmy

Řízení přístupu a více přenosových front klastru

Související úlohy

Přidání definice vzdálené fronty k izolování zpráv odeslaných ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá vzdálenou definici klastrované fronty a oddělený odesílací kanál a přenosovou frontu.

Přidání přenosové fronty klastru za účelem izolování přenosu zpráv klastru odeslaného ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá přídavnou přenosovou frontu klastru k oddělení zpráv o provozu zpráv jednomu správci front v klastru.

Přidání klastru a fronty vysílání klastru k izolování přenosu zpráv klastru odeslaného ze správce front brány
Upravte konfiguraci překrývajících se klastrů, které používají správce front brány. Po přenesení zpráv úprav do aplikace ze správce front brány bez použití stejné přenosové fronty nebo kanálů jako ostatní zprávy klastru. Řešení používá další klastr k izolování zpráv do konkrétní fronty klastru.

Klastrování: izolace aplikace pomocí více přenosových front klastru

Klastrování: Plánování konfigurace přenosových front klastru

“Přidání správce front do klastru: samostatné přenosové fronty” na stránce 290
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí více přenosových front klastru.

Odebrání fronty klastru ze správce front

Zakažte frontu INVENTQ v Torontu. Odešle všechny zprávy soupisu do New Yorku a odstraní frontu INVENTQ v Torontu, když je prázdná.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front, který je hostitelem fronty” na stránce 294. Obsahuje čtyři správce front. LONDON a NEWYORK obsahují úplná úložiště. PARIS a TORONTO obsahují dílčí úložiště. Aplikace inventáře se spouští na systémech v New Yorku a Torontu a je řízena přijetím zpráv ve frontě INVENTQ .
- Vzhledem ke snížení pracovní zátěže již nechcete spouštět aplikaci inventáře v Torontu. Chcete zakázat frontu INVENTQ , jejímž hostitelem je správce front TORONTO, a v produktu NEWYORKmají zprávy kanálu TORONTO ke frontám INVENTQ .
- Síťová konektivita existuje mezi všemi čtyřmi systémy.
- Síťový protokol je TCP.

Informace o této úloze

Chcete-li odebrat frontu klastru, postupujte takto.

Postup

1. Označuje, že fronta již není k dispozici.

   Chcete-li odebrat frontu z klastru, odeberte název klastru z definice lokální fronty. Pozměnit INVENTQ na TORONTO tak, aby nebyla přístupná ze zbytku klastru:

   ```
   ALTER QLOCAL(INVENTQ) CLUSTER(' ')
   ```

2. Zkontrolujte, zda již fronta není k dispozici.

   Ve správci front úplného úložiště, buď LONDON nebo NEWYORK, zkontrolujte, že fronta již není hostitelem správce front TORONTO zadáním následujícího příkazu:

   ```
   DIS QCLUSTER (INVENTQ)
   ```

   Příkaz TORONTO není uveden ve výsledcích, pokud byl příkaz ALTER úspěšně dokončen.

3. Zakažte frontu.

   Zakažte frontu INVENTQ na TORONTO tak, aby do ní nebyly zapsány žádné další zprávy:

   ```
   ALTER QLOCAL(INVENTQ) PUT(DISABLED)
   ```

   Nyní probíhá odesílání zpráv do této fronty pomocí příkazu MQOO_BIND_ON_OPEN do fronty nedoručených zpráv. Je třeba ukončit všechny aplikace, aby byly explicitně odesílány zprávy do fronty v tomto správci front.

4. Monitorujte frontu, dokud není prázdná.

   Monitorujte frontu pomocí příkazu DISPLAY QUEUE , uveďte atributy IPPROCS, OPPROCSa CURDEPTH, nebo použijte příkaz **WRKMQMSTS** na IBM i. Když je počet vstupních a výstupních procesů a aktuální hloubka queuesare nula, je fronta prázdná.

5. Monitorujte kanál, abyste se ujistili, že neexistují žádné nejisté zprávy.

Chcete-li se ujistit, že kanál INVENTORY.TORONTOneobsahuje žádné nejisté zprávy, sledujte kanál odesílatele klastru s názvem INVENTORY.TORONTO v každém z ostatních správců front. Zadejte příkaz DISPLAY CHSTATUS se zadáním parametru INDOUBT z každého správce front:

```
DISPLAY CHSTATUS(INVENTORY.TORONTO) INDOUBT
```

Pokud existují nějaké neověřené zprávy, musíte je vyřešit, než budete pokračovat. Například můžete zkusit vydat příkaz kanálu RESOLVE nebo zastavit a restartovat kanál.

6. Vymažte lokální frontu.

   Jste-li spokojeni s tím, že v produktu TORONTOnejsou k dispozici žádné další zprávy, které by bylo možné doručit do aplikace soupisu, můžete frontu odstranit:

```
DELETE QLOCAL(INVENTQ)
```

7. Nyní můžete odebrat aplikaci soupisu ze systému v Torontu

   Odebráním aplikace se vyhnete duplikaci a šetří místo na systému.

Výsledky

Klastr nastavený touto úlohou je stejný jako ten, který byl nastaven předchozí úlohou. Rozdíl je v tom, že fronta INVENTQ již není ve správci front TORONTOk dispozici.

Když jste v kroku 1 zanesli frontu ze služby, správce front produktu TORONTO odeslal zprávu do dvou správců front úplného úložiště. Informovali je o změně stavu. Správci front úplného úložiště předávají tyto informace ostatním správcům front v klastru, kteří požadovali aktualizace informací týkajících se konzoly INVENTQ.

Když správce front vloží zprávu do fronty produktu INVENTQ , aktualizované dílčí úložiště označuje, že fronta INVENTQ je k dispozici pouze ve správci front NEWYORK . Zpráva se odešle do správce front produktu NEWYORK .

Jak pokračovat dále

V této úloze byla pouze jedna fronta pro odebrání a pouze jeden klastr, ze kterého se má odebrat.

Předpokládejme, že existuje mnoho front odkazujících na seznam názvů obsahující mnoho názvů klastrů. Například správce front produktu TORONTO nemusí být hostitelem pouze produktu INVENTQ, ale také PAYROLLQ, SALESQa PURCHASESQ. Produkt TORONTO zpřístupňuje tyto fronty ve všech příslušných klastrech, INVENTORY, PAYROLL, SALESa PURCHASES. Definujte seznam názvů klastrů ve správci front produktu TORONTO :

```
DEFINE NAMELIST(TOROLIST)
DESCR('List of clusters TORONTO is in')
NAMES(INVENTORY, PAYROLL, SALES, PURCHASES)
```

Přidejte seznam názvů do každé definice fronty:

```
DEFINE QLOCAL(INVENTQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(PAYROLLQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(SALESQ) CLUSNL(TOROLIST)
DEFINE QLOCAL(PURCHASESQ) CLUSNL(TOROLIST)
```

Nyní předpokládejme, že chcete odebrat všechny tyto fronty z klastru SALES , protože operace SALES má být převzata operací PURCHASES . Vše, co musíte udělat, je změnit seznam názvů produktu TOROLIST a odebrat z něj název klastru SALES .

Chcete-li odebrat jednu frontu z jednoho z klastrů v seznamu názvů, vytvořte seznam názvů obsahující zbývající seznam názvů klastrů. Poté upravte definici fronty tak, aby používala nový seznam názvů. Chcete-li odebrat produkt PAYROLLQ z klastru INVENTORY , postupujte takto:

1. Vytvořte seznam názvů:

```
DEFINE NAMELIST(TOROSHORTLIST)
DESCR('List of clusters TORONTO is in other than INVENTORY')
NAMES(PAYROLL, SALES, PURCHASES)
```

2. Změňte definici fronty produktu PAYROLLQ :

```
ALTER QLOCAL(PAYROLLQ) CLUSNL(TOROSHORTLIST)
```

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 336.

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 288a upraven podle popisu v části “Odebrání fronty klastru ze správce front” na stránce 332.

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 298. 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 332.
   - 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 “Přesun definice tématu klastru do jiného správce front” na stránce 389.

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 288. 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 “Obnova správce front do stavu před klastrem” na stránce 338.

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 významnému problému systému nebo konfigurace nemůže správce front komunikovat s žádným úplným úložištěm v klastru.

Než začnete

Tato alternativní metoda odebrání správce front z klastru ručně zastaví a odstraní všechny kanály klastru propojující odebraného správce front s klastrem a vynutí odebrání správce front z klastru. Tato metoda se používá ve scénářích, kdy odebírané správce front nemůže komunikovat s žádným z úplných úložišť. To může být (například), protože správce front přestal pracovat, nebo protože došlo k delšímu komunikačnímu selhání mezi správcem front a klastrem. V opačném případě použijte nejběžnější metodu: “Odebrání správce front z klastru: doporučený postup” na stránce 334.

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 288a upraven podle popisu v části “Odebrání fronty klastru ze správce front” na stránce 332.

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 v případě nouze vhodný, nelze-li čekat na to, aby správce front opustil klastr hladce.

Postup

1. Před odebráním správce front z klastru se ujistěte, že správce front již není hostitelem prostředků potřebných pro klastr:
   - Pokud je správce front hostitelem úplného úložiště, proveďte kroky 1-6 z adresáře “Přesunutí úplného úložiště do jiného správce front” na stránce 298. 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 332.
   - 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 “Přesun definice tématu klastru do jiného správce front” na stránce 389.

     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 příkazu MODE(FORCE) lze kanál CLUSRCVR zastavit ve správci front LONDON. V opačném případě může být třeba počkat, až správce front odesílatele zastaví kanál:

   ```
   STOP CHANNEL(INVENTORY.LONDON) MODE(FORCE)
   STOP CHANNEL(INVENTORY.TORONTO)
   STOP CHANNEL(INVENTORY.PARIS)
   STOP CHANNEL(INVENTORY.NEWYORK)
   ```
3. Sledujte stavy kanálů ve správci front LONDONaž do zastavení kanálů:

   ```
   DISPLAY CHSTATUS(INVENTORY.LONDON)
   DISPLAY CHSTATUS(INVENTORY.TORONTO)
   DISPLAY CHSTATUS(INVENTORY.PARIS)
   DISPLAY CHSTATUS(INVENTORY.NEWYORK)
   ```

   Po zastavení kanálů se do ostatních správců front v klastru neodesílají žádné další zprávy aplikací.
4. Odstraňte ručně definované kanály klastru ve správci front LONDON:

   ```
   DELETE CHANNEL(INVENTORY.NEWYORK)
   DELETE CHANNEL(INVENTORY.TORONTO)
   ```
5. Zbývající správci front v klastru si stále uchovávají znalosti odebíraného správce front a mohou k němu i nadále odesílat zprávy. Chcete-li vymazat znalosti ze zbývajících správců front, resetujte odebraného správce front z klastru na jednom z úplných úložišť:

   ```
   RESET CLUSTER(INVENTORY) ACTION(FORCEREMOVE) QMNAME(LONDON) QUEUES(YES)
   ```

   Může-li existovat jiný správce front v klastru, který má stejný název jako odebraný správce front, zadejte **QMID** odebraného správce front.

Výsledky

Správce front LONDON již není součástí klastru. 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 šíření změn v celém klastru a do tohoto správce front nejsou doručovány žádné další zprávy, odstraňte kanál produktu CLUSRCVR v systému LONDON:

```
DELETE CHANNEL(INVENTORY.LONDON)
```

Odebraného správce front lze později přidat zpět do klastru, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 288. 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 “Obnova správce front do stavu před klastrem” na stránce 338.

Související odkazy

DELETE CHANNEL (odstranění kanálu)

DISPLAY CHANNEL (definice zobrazovaného kanálu)

ZOBRAZIT CHSTAV (Zobrazení stavu kanálu)

ZOBRAZIT CLUSQMGR (zobrazit informace o kanálu pro správce front klastru)

STOP CHANNEL (zastaví kanál)

RESET CLUSTER (reset klastru)

Obnova správce front do stavu před klastrem

Je-li správce front odebrán z klastru, uchovává informace o zbývajících členech klastru. Tyto znalosti nakonec vyprší a budou odstraněny automaticky. Pokud však chcete tuto akci odstranit okamžitě, můžete použít kroky uvedené v tomto tématu.

Než začnete

Předpokládá se, že správce front byl odebrán z klastru a že již neprovádí žádnou práci v klastru. Například, její fronty již nepřijímají zprávy z klastru a žádné aplikace nečekají na doručení zpráv do těchto front.

Informace o této úloze

Je-li správce front odebrán z klastru, uchovává znalosti o zbývajících členech klastru po dobu až 90 dnů. Může mít systémové výhody, zvláště pokud se správce front rychle znovu připojí ke klastru. Po konečném vypršení platnosti této znalosti dojde k automatickému odstranění tohoto souboru. Existují však důvody, proč byste měli raději tyto informace odstranit ručně. Příklad:

- Možná budete chtít potvrdit, že jste zastavili každou aplikaci v tomto správci front, která dříve používala prostředky klastru. Dokud nedojde k vypršení platnosti znalostí zbývajících členů klastru, bude každá taková aplikace pokračovat v zápisu do přenosové fronty. Po odstranění znalostí klastru systém vygeneruje chybovou zprávu, když se taková aplikace pokusí použít prostředky klastru.
- Zobrazíte-li informace o stavu správce front, můžete raději nezobrazovat informace o skončení platnosti zbývajících členů klastru.

Tato úloha používá klastr INVENTORY jako příklad. Správce front produktu LONDON byl odebrán z klastru INVENTORY , jak je popsáno v tématu “Odebrání správce front z klastru: doporučený postup” na stránce 334. Chcete-li odstranit informace o zbývajících členech klastru, zadejte ve správci front produktu LONDON následující příkazy.

Postup

1. Odeberte veškerou paměť ostatních správců front v klastru z tohoto správce front:

```
REFRESH CLUSTER(INVENTORY) REPOS(YES)
```

2. Monitorujte správce front, dokud nebudou všechny prostředky klastru pryč:

```
DISPLAY CLUSQMGR(*) CLUSTER(INVENTORY)
DISPLAY QCLUSTER(*) CLUSTER(INVENTORY)
DISPLAY TOPIC(*) CLUSTER(INVENTORY)
```

Související pojmy

Klastry

Porovnání klastrování a distribuovaných front

Komponenty klastru

Údržba správce front

Chcete-li provést údržbu, pozastavte a obnovte správce front z klastru.

Informace o této úloze

Čas od času může být nutné provést údržbu u správce front, který je součástí klastru. Například můžete potřebovat provést zálohování dat ve svých frontách nebo použít opravy na software. Pokud správce front je hostitelem jakýchkoli front, je třeba jeho aktivity pozastavit. Když je údržba dokončena, její aktivity mohou být obnoveny.

Postup

1. Pozastavit správce front zadáním příkazu SUSPEND QMGR **runmqsc** :

```
SUSPEND QMGR CLUSTER(SALES)
```

   Příkaz SUSPEND **runmqsc** oznamuje správci front v klastru SALES , že tento správce front byl pozastaven.

   Účelem příkazu SUSPEND QMGR je pouze informovat ostatní správce front, aby se vyhnuli odesílání zpráv do tohoto správce front, je-li to možné. Neznamená to, že správce front je zakázán. Některé zprávy, které mají být zpracovány tímto správcem front, jsou stále k sobě odeslány, například když je tento správce front jediným hostitelem klastrované fronty.

   Když je správce front pozastaven, rutiny správy pracovní zátěže se vyhnou odesílání zpráv do tohoto modulu. Zprávy, které mají být zpracovány tímto správcem front, zahrnují zprávy odeslané lokálním správcem front.

   IBM MQ používá algoritmus vyrovnávání pracovní zátěže k určení toho, která místa určení jsou vhodná, místo toho, aby bylo možné kdykoli vybrat lokálního správce front.

   a) Vynucení pozastavení správce front pomocí volby FORCE v příkazu SUSPEND QMGR :

```
SUSPEND QMGR CLUSTER(SALES) MODE(FORCE)
```

      Produkt MODE(FORCE) vynutí zastavení všech příchozích kanálů od jiných správců front v klastru. Pokud nezadáte MODE(FORCE), použije se výchozí MODE(QUIESCE) .

2. Proveďte všechny úlohy údržby potřebné.
3. Obnovte správce front zadáním příkazu RESUME QMGR **runmqsc** :

```
RESUME QMGR CLUSTER(SALES)
```

Výsledky

Příkaz RESUME **runmqsc** upozorňuje na úplná úložiště, která je správce front k dispozici znovu. Správci front úplného úložiště šíří tyto informace do jiných správců front, kteří požádali o aktualizace informací o tomto správci front.

Údržba přenosové fronty klastru

Učinit veškeré úsilí, aby byly k dispozici přenosové fronty klastru. Jsou nezbytné pro výkon klastrů.

z/OS V z/OSnastavte INDXTYPE přenosové fronty klastru na CORRELID.

Než začnete

- Ujistěte se, že se přenosová fronta klastru nezaplní.
- Dávejte pozor, abyste nevydali příkaz ALTER **runmqsc** k nastavení, ať se deaktivuje nebo deaktivuje omylem.
- Ujistěte se, že médium přenosové fronty klastru je uloženo v z/OS (například z/OS sad stránek) , nebude zaplněno.

Informace o této úloze

z/OS

Následující procedura se vztahuje pouze na z/OS.

Postup

Nastavte INDXTYPE přenosové fronty klastru na CORRELID

Obnova správce front klastru

Pomocí příkazu REFRESH CLUSTER lze odebrat automaticky definované kanály a automaticky definované objekty klastru z lokálního úložiště. Žádné zprávy nejsou ztraceny.

Než začnete

Můžete být požádáni o použití příkazu pro centrum podpory produktu IBM . Nepoužívejte tento příkaz bez důkladného uvážení. Například u velkých klastrů pomocí příkazu **REFRESH CLUSTER** může dojít k přerušení činnosti klastru při jeho průběhu, a poté znovu ve 27. denních intervalech, když objekty klastru automaticky odesílají aktualizace stavu všem zúčastněným správcům front. Viz Klastrování: Použití doporučených postupů REFRESH CLUSTER.

Informace o této úloze

Správce front může vytvořit nový začátek v klastru. Za normálních okolností není třeba použít příkaz REFRESH CLUSTER .

Postup

Zadáním příkazu REFRESH CLUSTER **MQSC** ze správce front odeberte automaticky definované objekty správce front klastru a fronty z lokálního úložiště.

Tento příkaz pouze odebere objekty, které odkazují na jiné správce front, neodebere objekty související s lokálním správcem front. Příkaz také odebere automaticky definované kanály. Odebírá kanály, které nemají zprávy v přenosové frontě klastru a nejsou připojeny k úplnému správci front úložiště.

Výsledky

Ve skutečnosti příkaz REFRESH CLUSTER umožňuje, aby správce front byl studený s ohledem na obsah celého úložiště. Produkt IBM MQ zajišťuje, že ve frontách nebudou ztracena žádná data.

Související informace
Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Obnova správce front klastru

Pomocí příkazu REFRESH CLUSTER **runmqsc** převeďte informace o klastru do aktuálního správce front až do data. Postupujte podle této procedury po obnovení správce front z bodu v časovém okamžiku.

Než začnete

Obnovili jste správce front klastru ze zálohy k určitému časovému bodu.

Informace o této úloze

Chcete-li obnovit správce front v klastru, obnovte správce front a poté uveďte informace o klastru do data pomocí příkazu REFRESH CLUSTER **runmqsc** .

Poznámka: 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 v obnoveném správci front pro všechny klastry, jichž se správce front účastní.

Jak pokračovat dále

V žádném jiném správci front není třeba zadávat příkaz REFRESH CLUSTER .

Související informace
Klastrování: Využití doporučených postupů pro příkaz REFRESH CLUSTER

Konfigurace kanálů klastru pro dostupnost

Postupujte podle správných postupů konfigurace, aby kanály klastru běžela bez problémů, pokud existují přerušované zastavování sítě.

Než začnete

Klastry vás zbavují nutnosti definovat kanály, ale přesto je musíte udržovat. Stejná technologie kanálu se používá pro komunikaci mezi správci front v klastru tak, jak se používá v distribuovaných frontách. Chcete-li porozumět kanálům klastru, musíte být obeznámeni s otázkami, jako jsou například:

- Způsob fungování kanálů
- Jak zjistit jejich stav
- Jak používat uživatelské procedury kanálu

Informace o této úloze

Možná byste měli věnovat zvláštní pozornost následujícím bodům:

Postup

Při konfiguraci kanálů klastru zvažte následující body

- Vyberte hodnoty pro HBINT nebo KAINT na odesílacích kanálech klastru a přijímacích kanálech klastru, které nezatěžují síť se spoustou synchronizačních signálů nebo s udržováním živých toků. Interval kratší než přibližně 10 sekund dává falešné selhání, pokud se vaše síť někdy zpomaluje a zavádí zpoždění této délky.
- Nastavte hodnotu parametru BATCHHB tak, aby se okno snížilo, protože je to nejisté, protože je to u kanálu, u kterého došlo k selhání. Nejistá dávka na kanálu, u kterého došlo k selhání, se bude pravděpodobně vyskytnout v případě, že je dávka již zaplněn. Je-li provoz zpráv v rámci kanálu sporadický s dlouhými časovými úseky mezi shlukováním zpráv, je pravděpodobnější, že je dávka neúspěšná.
- Problém vzniká tehdy, když se konec kanálu odesílatele klastru nezdaří a poté se pokusí o restartování před tím, než prezenční signál nebo udržení aktivity zjistí selhání. Restart channel-sender je odmítnut, pokud byl konec kanálu klastru, který byl příjemcem aktivní, aktivní. Chcete-li se vyhnout selhání, zařiďte, aby se kanál příjemce klastru ukončil a restartoval, když se kanál odesílatele klastru pokusí o restart.

  z/OS **zapIBM MQ for z/OS**
  Řídí problém konce příjemce klastru, který zůstává aktivní pomocí parametrů ADOPTMCA a ADOPTCHK v systému ALTER QMGR.

  Multi **zapMultiplatforms**
  Řídí problém konce příjemce klastru, který zůstává aktivní pomocí atributů AdoptNewMCA, AdoptNewMCATimeouta AdoptNewMCACheck v souboru qm.ini nebo v registru Windows NT .

Kontrola, zda byly ukončeny asynchronní příkazy pro distribuované sítě

Mnoho příkazů je asynchronní, je-li použito v distribuované síti. V závislosti na příkazu a stavu sítě, když je vydán, může trvat mnoho času dokončení. Správce front zprávu o dokončení nevydá, takže potřebujete další způsoby kontroly, zda byl příkaz dokončen.

Informace o této úloze

Téměř každá změna konfigurace, kterou provedete na klastru, pravděpodobně bude asynchronně dokončena. Důvodem je vnitřní administrace a aktualizace cyklů, které fungují v rámci klastrů. U hierarchií typu publikování/odběr se jakákoli změna konfigurace, která ovlivní odběry, pravděpodobně asynchronně dokončí. To není vždy zřejmé z názvu příkazu.

Všechny následující příkazy MQSC mohou být asynchronně dokončeny. 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 autobusových sítí. Příkaz **REFRESH CLUSTER** může trvat mnohem delší dobu, zvláště když je současně vydán více správců front.

Chcete-li mít jistotu, že tyto příkazy byly dokončeny, zkontrolujte, zda existují očekávané objekty ve vzdálených správcích front.

Procedura

- ALTER QMGR

  V případě příkazu ALTER QMGR PARENT použijte příkaz DISPLAY PUBSUB TYPE(PARENT) ALL ke sledování stavu požadovaného nadřízeného vztahu.

  U příkazů 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 Parametry ALTER CHANNELpoužijte příkaz DISPLAY CLUSQMGR k monitorování změny, když byly změny šířeny do klastru.
- DEFINE NAMELIST, ALTER NAMELISTa DELETE NAMELIST.

Pokud použijete parametr **NAMELIST** v atributu **CLUSNL** objektu **QMgr** , může tento objekt ovlivnit fronta nebo kanál klastru. Monitor je vhodný pro ovlivněný objekt.

Změny na SYSTEM.QPUBSUB.QUEUE.NAMELIST mohou ovlivnit vytvoření nebo zrušení proxy odběrů v hierarchii publikování/odběru. Použijte příkaz DISPLAY SUB SUBTYPE(PROXY) k monitorování tohoto.

- DEFINE front, ALTER queuesa DELETE queues.

  Pro všechny parametry uvedené v tabulce Parametry, které lze vrátit příkazem DISPLAY QUEUE, použijte příkaz DISPLAY QCLUSTER k monitorování změny, když byly změny šířeny do klastru.

- DEFINE SUBa DELETE SUB

  Definujete-li první odběr 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 odběry proxy v hierarchii publikování/odběru nebo v klastru publikování/odběru.

  Chcete-li zkontrolovat, zda byl dokončen příkaz definující nebo odstranění odběru, zkontrolujte, zda očekávaný odběr serveru proxy existuje na jiných správcích front v distribuované síti, či nikoli. Používáte-li v klastru *přímé směrování* , zkontrolujte, zda v ostatních dílčích úložištích v klastru existuje očekávaný odběr serveru proxy. Používáte-li *směrování hostitele témat* v klastru, zkontrolujte, zda existuje očekávaný odběr serveru proxy na odpovídajících hostitelích témat. Použijte následující příkaz MQSC:

  ```
  DISPLAY SUB(*) SUBTYPE(PROXY)
  ```

  Při vydávání v klastru nebo hierarchii použijte stejnou kontrolu pro následující ekvivalentní volání MQI odběru a odběru zpráv o zrušení odběru:

  – Přihlaste se k odběru pomocí příkazu MQSUB.
  – Zrušte přihlášení s použitím MQCLOSE s MQCO_REMOVE_SUB.

- DEFINE TOPIC, ALTER TOPICa DELETE TOPIC

  Chcete-li zkontrolovat, zda byla dokončena definice příkazu definující, pozměňující nebo odstraňující klastrované téma, zobrazte téma v jiných dílčích úložištích v klastru (pokud používáte *přímé směrování*). nebo na ostatních hostitelích témat (používáte-li *směrování hostitele témat*).

  Pro všechny parametry uvedené v tabulce Parametry, které lze vrátit příkazem DISPLAY TOPIC, použijte příkaz DISPLAY TCLUSTER k monitorování změny, když byly změny šířeny do klastru.

  Poznámka:

  – Parametr **CLUSTER** může ovlivnit vytvoření nebo zrušení proxy odběrů v klastru publikování/odběru.
  – Parametry **PROXYSUB** a **SUBSCOPE** mohou ovlivnit vytváření nebo zrušení proxy odběrů v rámci hierarchie publikování/odběru nebo klastru publikování/odběru.
  – Použijte příkaz DISPLAY SUB SUBTYPE(PROXYSUB) k monitorování tohoto.

- Aktualizovat klastr

  Pokud spouštíte příkaz **REFRESH CLUSTER** , zadejte výzvu do hloubky fronty příkazů klastru. Před vyhledáním objektů počkejte, až se dosáhne nuly, a zůstane na nule.

  1. Pomocí následujícího příkazu MQSC zkontrolujte, zda je hloubka fronty příkazů klastru nulová.

     ```
     DISPLAY QL(SYSTEM.CLUSTER.COMMAND.QUEUE) CURDEPTH
     ```

  2. Zopakujte kontrolu, dokud hloubka fronty nedosáhne nuly, a zůstane na nule v následné kontrole.

  Příkaz **REFRESH CLUSTER** odstraní a znovu vytvoří objekty a 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. Pokud používáte *směrování hostitele témat* v klastru, zkontrolujte, zda byly očekávané odběry proxy 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 příkaz DISPLAY CLUSQMGR.
- RESET QMGR TYPE (PUBSUB)

  Chcete-li zkontrolovat, zda byl příkaz **RESET QMGR** dokončen, použijte příkaz DISPLAY PUBSUB TYPE(PARENT|CHILD).

  Poznámka: Příkaz **RESET QMGR** může způsobit zrušení proxy odběrů v hierarchii publikování/odběru nebo v klastru publikování/odběru. Použijte příkaz DISPLAY SUB SUBTYPE(PROXYSUB) k monitorování tohoto.
- Možná budete chtít monitorovat také další systémové fronty, které, jak a kdy jsou dokončené, směřují k hloubce fronty nula.

  Můžete například chtít monitorovat frontu SYSTEM.INTER.QMGR.CONTROL a frontu SYSTEM.INTER.QMGR.FANREQ . Viz Monitorování přenosů odběru proxy odběrů v klastrech a Vyvážení výrobců a odběratelů v sítích typu publikování/odběr.

Jak pokračovat dále

Pokud tyto kontroly nepotvrdí, že byl asynchronní příkaz dokončen, může se vyskytnout chyba. Chcete-li vyšetřit, nejprve zkontrolujte protokol správce front, ve kterém byl příkaz zadán, potom (pro klastr) zkontrolujte protokoly úplného úložiště klastru.

Související odkazy

z/OS Asynchronní chování příkazů CLUSTER v systému z/OS

Směrování zpráv do a z klastrů

Aliasy fronty, aliasy správců front a definice vzdálených front slouží k připojení klastrů k externím správcům front a dalším klastrům.

Podrobnosti o směrování zpráv do a z klastrů naleznete v následujících dílčích tématech:

Související pojmy

Klastry

Porovnání klastrování a distribuovaných front

Komponenty klastru

“Aliasy správce front a klastry” na stránce 358

Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

“Aliasy front a klastry” na stránce 361

Aliasy front použijte ke skrytí názvu fronty klastru, ke klastrování fronty, převzetí různých atributů nebo převzetí různých řízení přístupu.

“Aliasy fronty pro odpověď a klastry” na stránce 360

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí lze použít s klastry stejně jako v prostředí distribuovaných front.

Související úlohy

“Konfigurace klastru správce front” na stránce 265

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 277
Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

Konfigurace požadavku/odpovědi na klastr
Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

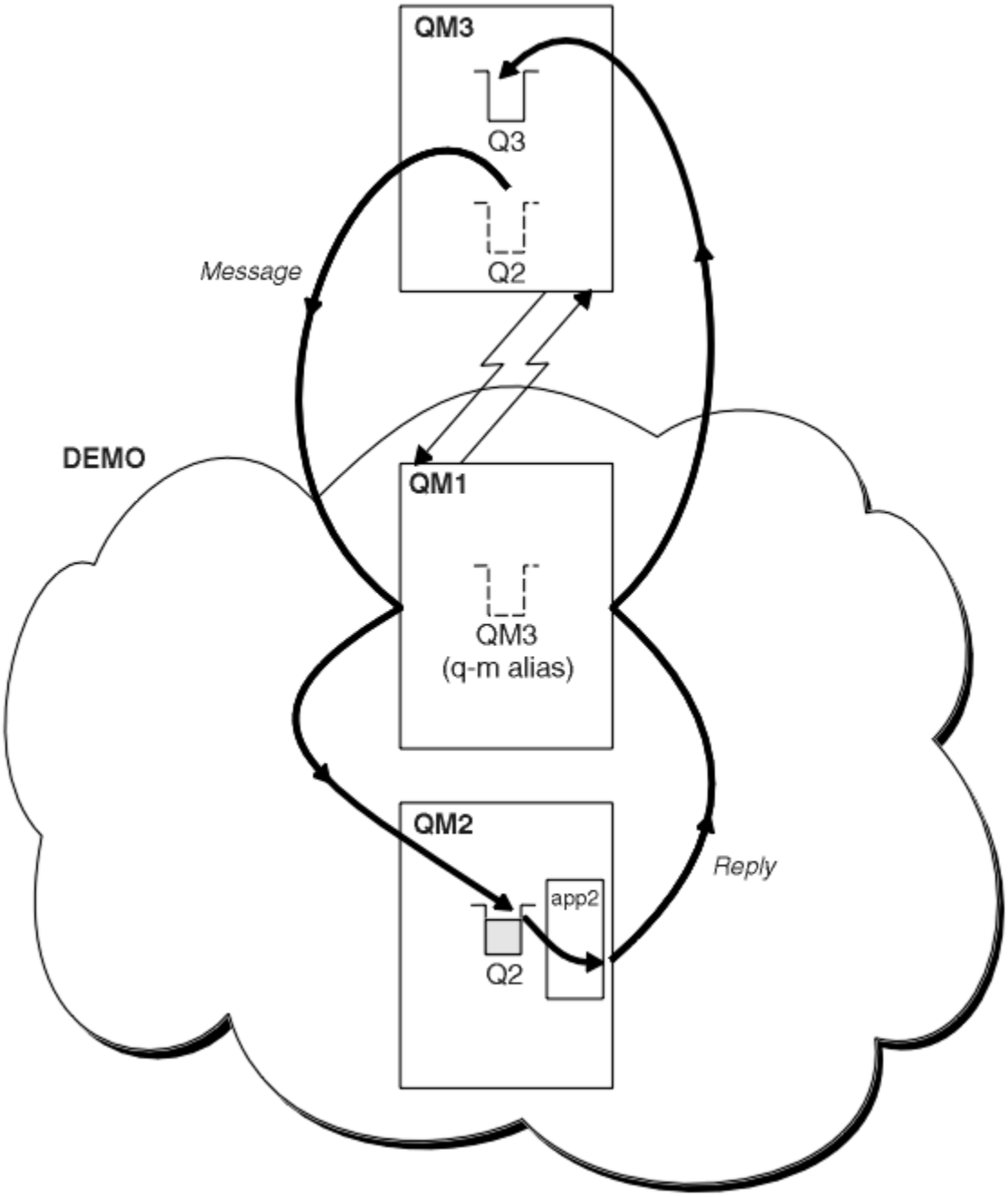
Než začnete

Produkt Obrázek 55 na stránce 346 zobrazuje správce front s názvem QM3 , který se nachází mimo klastr s názvem DEMO. QM3 může být správce front na produktu IBM MQ , který nepodporuje klastry. QM3 je hostitelem fronty s názvem Q3, která je definována takto:

```
DEFINE QLOCAL(Q3)
```

Uvnitř klastru jsou dva správci front s názvem QM1 a QM2. Produkt QM2 je hostitelem fronty klastru s názvem Q2, která je definována takto:

```
DEFINE QLOCAL(Q2) CLUSTER(DEMO)
```



Obrázek 55. Vložení ze správce front mimo klastr

Informace o této úloze

Chcete-li nastavit cestu pro zprávy požadavku a odpovědi, postupujte podle pokynů v proceduře.

Postup

1. Odešlete zprávu požadavku do klastru.

   Zvažte, jakým způsobem správce front, který je mimo klastr, vloží zprávu do fronty Q2 na QM2, která je uvnitř klastru. Správce front mimo klastr musí mít definici QREMOTE pro každou frontu v klastru, do které umisťuje zprávy.

   a) Definujte vzdálenou frontu pro Q2 v systému QM3.

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(QM2) XMITQ(QM1)
```

Protože produkt QM3 není součástí klastru, musí komunikovat s použitím distribuovaných technik řazení do fronty. Proto musí mít také odesílací kanál a přenosovou frontu na QM1. Produkt QM1 potřebuje odpovídající přijímací kanál. Kanály a přenosové fronty nejsou explicitně zobrazeny v produktu Obrázek 55 na stránce 346.

V tomto příkladu aplikace v produktu QM3 vydá výzvu MQPUT k vložení zprávy do produktu Q2. Definice QREMOTE způsobí, že se zpráva bude směrována do Q2 v QM2 pomocí odesílacího kanálu, který získává zprávy z přenosové fronty QM1 .

2. Přijmout zprávu odpovědi z klastru.

   Alias správce front slouží k vytvoření návratové cesty pro odpovědi na správce front mimo klastr. Brána, QM1, oznamuje alias správce front pro správce front, který je mimo klastr, QM3. Potvrdí produkt QM3 správcům front v rámci klastru přidáním atributu klastru do definice aliasu správce front produktu QM3. Definice aliasu správce front je jako definice vzdálené fronty, ale s prázdnou hodnotou RNAME.

   a) Definujte alias správce front pro produkt QM3 v systému QM1.

   ```
   DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
   ```

   Musíme zvážit volbu názvu přenosové fronty použité k předání odpovědí zpět z produktu QM1 do produktu QM3. Implicitně v definici QREMOTE je při vynechání atributu XMITQ název přenosové fronty QM3. Ale QM3 je stejný název, jaký očekáváme, že inzerovat na zbytek klastru pomocí aliasu správce front. Produkt IBM MQ neumožňuje zadat název přenosové fronty i alias správce front se stejným názvem. Jedním z řešení je vytvoření přenosové fronty pro předávání zpráv do produktu QM3 s jiným názvem než alias správce front.

   b) Zadejte název přenosové fronty do definice QREMOTE .

   ```
   DEFINE QREMOTE(QM3) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO) XMITQ(QM3.XMIT)
   ```

   Alias nového správce front spojuje novou přenosovou frontu s názvem QM3.XMIT s aliasem správce front QM3 . Je to jednoduché a správné řešení, ale ne zcela uspokojivé. Porušeno konvence pojmenování pro přenosové fronty, které mají stejný název jako cílový správce front. Existují nějaká alternativní řešení, která zachovávají konvence pojmenování přenosových front?

   Problém vzniká, protože žadatel standardně předává QM3 jako název správce front odpovědi ve zprávě s požadavkem, který je odeslán z produktu QM3. Server v produktu QM2 používá název správce front pro odpověď QM3 na adresu QM3 ve svých odpovědích. Řešení požaduje produkt QM1 k inzerování produktu QM3 jako alias správce front, aby vrátil zprávy s odpovědí a zabránil produktu QM1 v používání produktu QM3 jako názvu přenosové fronty.

   Místo toho, aby jako výchozí název správce front byl zadán QM3 jako název správce front odpovědi, musí aplikace v produktu QM3 předat alias odpovědi správce front produktu QM1 pro zprávy odpovědí. Správce front brány QM1 inzeruje alias správce front pro odpovědi na QM3 spíše než o samotnou QM3 a vyhýbá se konfliktu s názvem přenosové fronty.

   c) Definujte alias správce front pro produkt QM3 v systému QM1.

   ```
   DEFINE QREMOTE(QM3.ALIAS) RNAME(' ') RQMNAME(QM3) CLUSTER(DEMO)
   ```

   Jsou vyžadovány dvě změny konfiguračních příkazů.

   i) Produkt QREMOTE v QM1 nyní oznamuje svůj alias správce front QM3.ALIAS zbytku klastru a pojmenuje jej na název skutečného správce front QM3. QM3 je znovu název přenosové fronty, která má odeslat fronty odpovědí zpět na QM3

ii) Klientská aplikace musí poskytovat `QM3.ALIAS` jako název správce front pro odpovědi, když vytváří zprávu požadavku. `QM3.ALIAS` klientské aplikaci můžete poskytnout dvěma způsoby aplikaci klienta.

- Kód `QM3.ALIAS` je v poli názvu správce front pro odpověď sestaveno pomocí `MQPUT` v `MQMD`. Musíte to provést tímto způsobem, pokud používáte dynamickou frontu pro odpovědi.
- Při zadávání názvu fronty pro odpověď použijte alias fronty k odpovědi, `Q3.ALIAS`, spíše než frontu pro odpověď.

```
DEFINE QREMOTE(Q3.ALIAS) RNAME(Q3) RQMNAME(QM3.ALIAS)
```

Jak pokračovat dále

Poznámka: Nemůžete demonstrovat použití aliasů fronty odpovědí s **AMQSREQ0**. Otevře frontu pro odpověď s použitím názvu fronty uvedeného v parametru 3 nebo ve výchozí modelové frontě produktu `SYSTEM.SAMPLE.REPLY` . Musíte upravit ukázku poskytující jiný parametr obsahující alias fronty pro odpověď pro pojmenování alias správce front pro produkt `MQPUT`pro odpověď.

Související pojmy

Aliasy správce front a klastry
Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy fronty pro odpověď a klastry
Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí 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 s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry
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 cílového správce front klastru” na stránce 348
Zasměrujte zprávu do fronty klastru, která je definovaná na libovolném správci front v klastru, aniž byste pojmenovali správce front.

Skrytí názvu cílového správce front klastru
Zasměrujte zprávu do fronty klastru, která je definovaná na libovolném správci front v klastru, aniž byste pojmenovali správce front.

Než začnete

- Vyhněte se odhalení názvů správců front, kteří jsou v klastru, ke správcům front, kteří nejsou členy klastru.
  - Vyřešení odkazů na správce front, který je hostitelem fronty v klastru, odebere flexibilitu při vyrovnávání pracovní zátěže.
  - Také je pro vás obtížné změnit správce front, který je hostitelem fronty v klastru.

  - Alternativou je nahradit parametr RQMNAME aliasem správce front poskytnutým administrátorem klastru.
  - Produkt “Skrytí názvu cílového správce front klastru” na stránce 348 popisuje použití aliasu správce front k odpojení správce front mimo klastr ze správy správců front v rámci klastru.
- Navrhovaným způsobem, jak pojmenovat přenosové fronty, je však poskytnout jim název cílového správce front. Název přenosové fronty odhaluje název správce front v klastru. Musíte zvolit, které pravidlo chcete sledovat. Název přenosové fronty můžete pojmenovat buď pomocí názvu správce front, nebo pomocí názvu klastru:

  Pojmenujte přenosovou frontu s použitím názvu správce front brány
  Zveřejňování názvu správce front brány pro správce front mimo klastr je vhodnou výjimkou pravidla skrývání názvů správců front klastru.

  Pojmenujte přenosovou frontu s použitím názvu klastru.
  Pokud se nekonvencí pojmenování přenosových front pojmenováváte pomocí názvu cílového správce front, použijte název klastru.

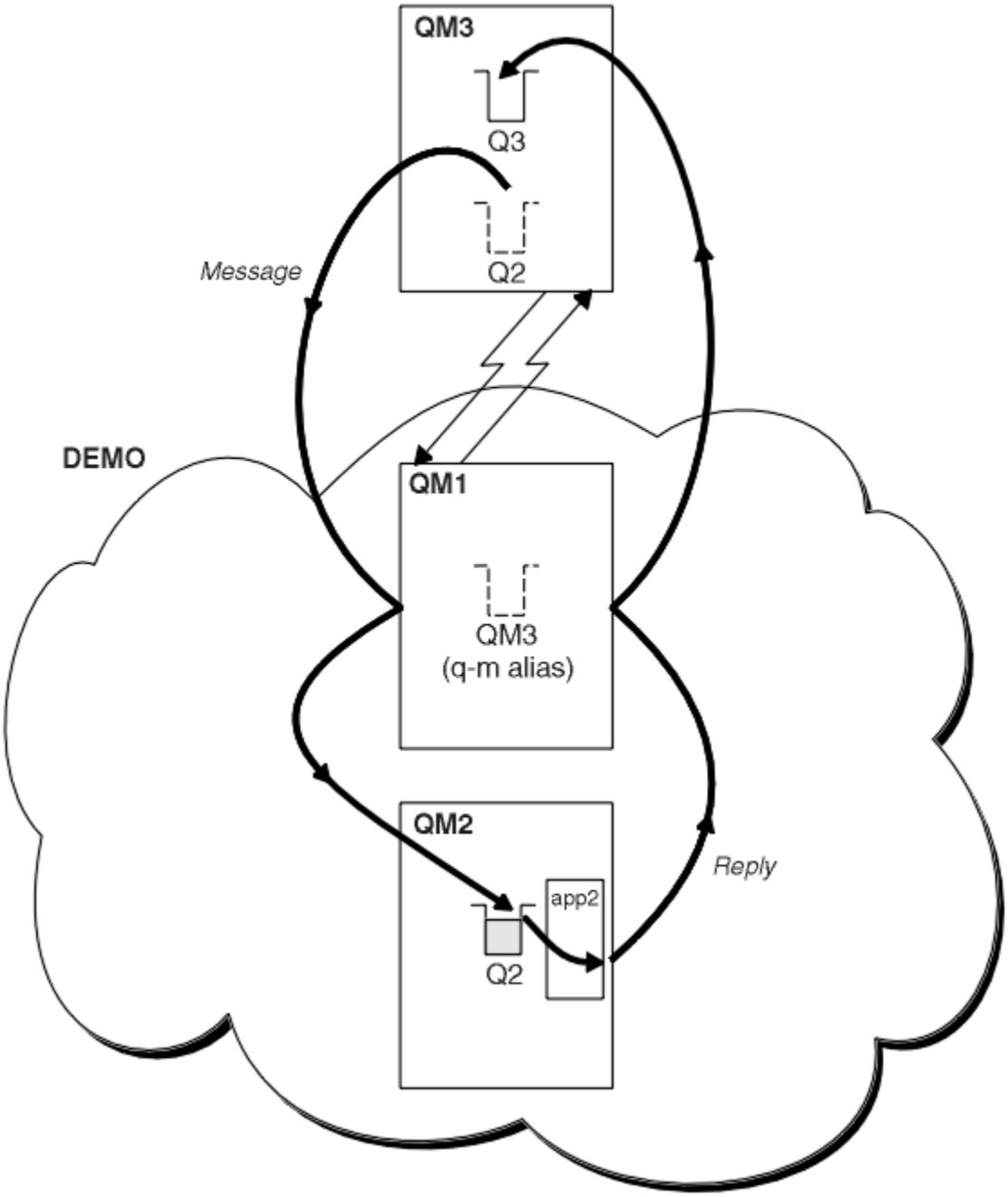
Informace o této úloze

Upravte úlohu “Konfigurace požadavku/odpovědi na klastr” na stránce 345tak, abyste skryli název cílového správce front v rámci klastru.

Postup

V tomto příkladu si prohlédněte téma Obrázek 56 na stránce 350, definujte alias správce front ve správci front brány QM1 s názvem DEMO:

```
DEFINE QREMOTE(DEMO) RNAME(' ') RQMNAME(' ')
```



Obrázek 56. Vložení ze správce front mimo klastr

Definice QREMOTE v systému QM1 způsobí, že správce front DEMO alias správce front je znám jako správce front brány. QM3, správce front mimo klastr může pomocí aliasu správce front DEMO odesílat zprávy do klastrovaných front v produktu DEMOmísto toho, aby bylo nutné použít skutečné jméno správce front.

Pokud převezmou konvenci použití názvu klastru k pojmenování přenosové fronty připojující se ke klastru, stane se definice vzdálené fronty pro produkt Q2 :

```
DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(DEMO) XMIT(DEMO)
```

Výsledky

Zprávy určené pro Q2 v umístění DEMO jsou umístěny do přenosové fronty DEMO . Z přenosové fronty jsou přenášeny odesílacím kanálem do správce front brány, QM1. Správce front brány směruje zprávy do libovolného správce front v klastru, který je hostitelem fronty klastru Q2.

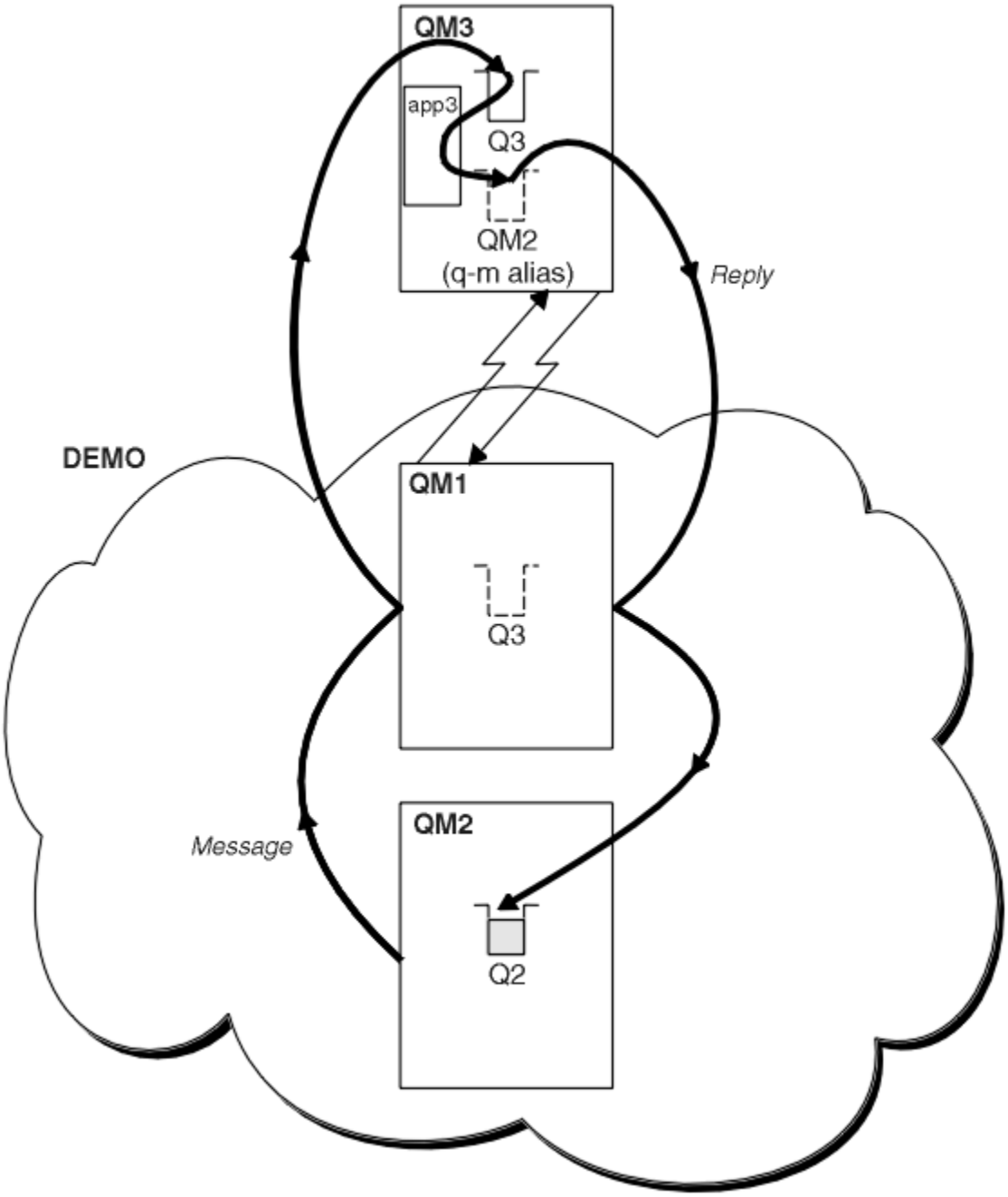
Konfigurace požadavku/odpovědi z klastru

Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Než začnete

Obrázek 57 na stránce 352 zobrazuje správce front QM2, uvnitř klastru DEMO. Odešle požadavek do fronty Q3, jehož hostitelem je správce front mimo klastr. Odpovědi jsou vraceny produktu Q2 v umístění QM2 v klastru.

Chcete-li komunikovat se správcem front mimo klastr, jeden nebo více správců front v rámci klastru se chová jako brána. Správce front brány má komunikační cestu ke správcům front mimo klastr. V tomto příkladu je QM1 brána.



Obrázek 57. Uvedení do správce front mimo klastr

Informace o této úloze

Postupujte podle pokynů pro nastavení cesty pro zprávy požadavku a odpovědi

Postup

1. Odešlete zprávu požadavku z klastru.

   Zvažte, jakým způsobem správce front QM2, který je uvnitř klastru, vloží zprávu do fronty Q3 v QM3, která je mimo klastr.

   a) Vytvořte definici QREMOTE na QM1 , která oznamuje vzdálenou frontu Q3 do klastru.

```
DEFINE QREMOTE(Q3) RNAME(Q3) RQMNAME(QM3) CLUSTER(DEMO)
```

Má také odesílací kanál a přenosovou frontu ke správci front, který je mimo klastr. QM3 má odpovídající přijímací kanál. Kanály nejsou zobrazeny v Obrázek 57 na stránce 352.

Aplikace v systému QM2 vydává volání MQPUT určující cílovou frontu a frontu, do níž mají být odesílány odpovědi. Cílová fronta je Q3 a fronta odpovědí je Q2.

Zpráva se odešle na server QM1, který používá svou definici vzdálené fronty k vyřešení názvu fronty do produktu Q3 v QM3.

2. Přijmout zprávu odpovědi od správce front mimo klastr.

   Správce front mimo klastr musí mít alias správce front pro každého správce front v klastru, do kterého má odeslat zprávu. Alias správce front musí také určovat název přenosové fronty ke správci front brány. V tomto příkladu produkt QM3 potřebuje definici aliasu správce front pro produkt QM2:

   a) Vytvořit alias správce front QM2 v systému QM3

   ```
   DEFINE QREMOTE(QM2) RNAME(' ') RQMNAME(QM2) XMITQ(QM1)
   ```

   Produkt QM3 také potřebuje odesílací kanál a přenosovou frontu pro QM1 a QM1 potřebuje odpovídající přijímací kanál.

   Aplikace, **app3**, na QM3 může potom odesílat odpovědi na QM2, zadáním volání MQPUT a zadáním názvu fronty, Q2 a názvu správce front QM2.

Jak pokračovat dále

Můžete definovat více než jednu trasu z klastru.

Související pojmy

Aliasy správce front a klastry
Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy fronty pro odpověď a klastry
Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí 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
Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry
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

Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Než začnete

Nakonfigurujte příklad, jak je zobrazeno v Obrázek 55 na stránce 346 v “Konfigurace požadavku/odpovědi na klastr” na stránce 345.

Informace o této úloze

V tomto scénáři správce front mimo klastr, QM3 v Obrázek 58 na stránce 355, odesílá požadavky do fronty Q2. Q2 je hostován na dvou správcích front, QM2 a QM4 v rámci klastru DEMO. Oba správci front jsou konfigurováni s volbou výchozí vazby NOTFIXED , aby bylo možné použít vyrovnávání pracovní zátěže. Požadavky z produktu QM3, správce front mimo klastr, jsou odeslány do instance produktu Q2 prostřednictvím produktu QM1.

QM3 není součástí klastru a komunikuje pomocí technik distribuovaných front. Musí mít odesílací kanál a přenosovou frontu na QM1. Produkt QM1 potřebuje odpovídající přijímací kanál. Kanály a přenosové fronty nejsou explicitně zobrazeny v produktu Obrázek 58 na stránce 355.

Procedura rozšiřuje příklad v produktu Obrázek 55 na stránce 346 v produktu “Konfigurace požadavku/odpovědi na klastr” na stránce 345.

Postup

1. Vytvořte definici QREMOTE pro Q2 na QM3.

   ```
   DEFINE QREMOTE(Q2) RNAME(Q2) RQMNAME(Q3) XMITQ(QM1)
   ```

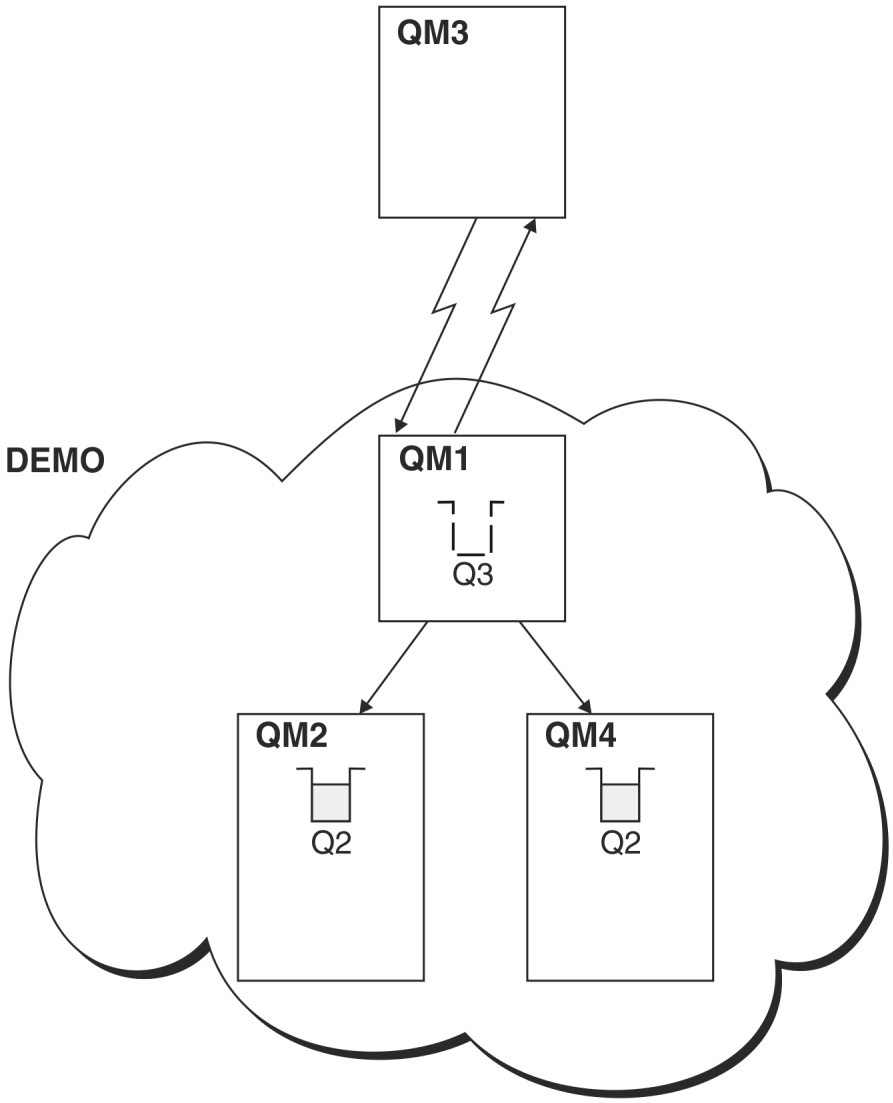
   Vytvořte definici QREMOTE pro každou frontu v klastru, do které produkt QM3 vkládá zprávy.
2. Vytvořte alias správce front Q3 v systému QM1.

   ```
   DEFINE QREMOTE(Q3) RNAME(' ') RQMNAME(' ')
   ```

   Q3 není název skutečného správce front. Jedná se o název definice aliasu správce front v klastru, který odpovídá názvu aliasu správce front Q3 s prázdnou hodnotou ' ' .
3. Definujte lokální frontu s názvem Q2 na každém z QM2 a QM4.

   ```
   DEFINE QLOCAL(Q2) CLUSTER(DEMO) DEFBIND(NOTFIXED)
   ```
4. QM1, nemá správce front brány žádné speciální definice.

Výsledky



Obrázek 58. Vložení ze správce front mimo klastr

Když aplikace v QM3 vyvolá výzvu MQPUT k vložení zprávy do Q2, definice QREMOTE na QM3 způsobí, že zpráva bude směrována přes správce front brány QM1. Když produkt QM1 přijme zprávu, je si vědom toho, že zpráva je stále zamýšlena pro frontu s názvem Q2 a provádí rozlišení názvu. Produkt QM1 kontroluje lokální definice a nenalezl nic pro Q2. Produkt QM1 poté zkontroluje konfiguraci klastru a zjistí, že je informován o dvou instancích produktu Q2 v klastru DEMO. Produkt QM1 může nyní využívat vyrovnávání pracovní zátěže k distribuci zpráv mezi instancemi portálu Q2 umístěnými na QM2 a QM4.

Související pojmy

Aliasy správce front a klastry
Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy fronty pro odpověď a klastry
Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí 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
Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace cest zpráv mezi klastry
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 informace

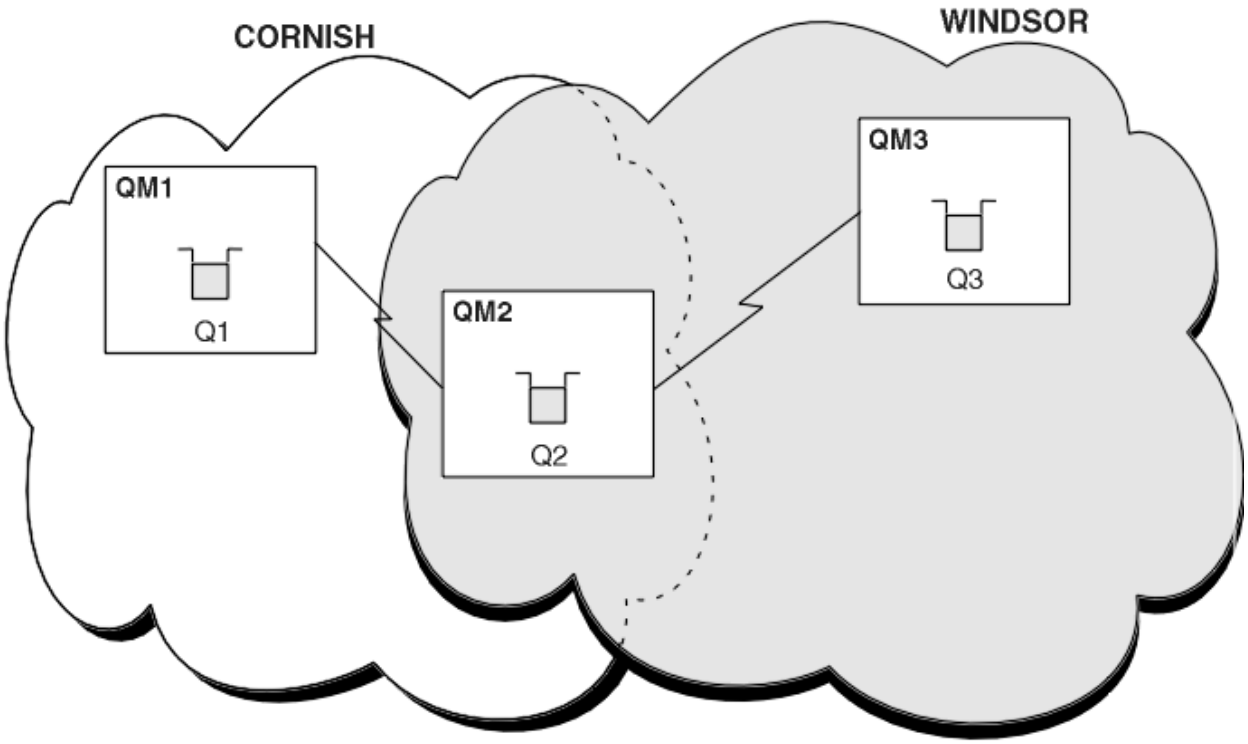
Rozlišení názvu fronty
Rozpoznání názvu

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 59. Přemostění mezi klastry

Obrázek 59 na stránce 356 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 59 na stránce 356v 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 správce front a klastry
Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy fronty pro odpověď a klastry
Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí 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
Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Aliasy správce front a klastry

Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy správce front, které jsou vytvořeny s použitím definice vzdálených front s mezerou RNAME, mají pět použití:

Přemapování názvu správce front při odesílání zpráv

Alias správce front lze použít k přemapování názvu správce front určeného ve volání MQOPEN na jiného správce front. Může se jednat o správce front klastru. Například správce front může mít 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, která provedla tuto definici, vloží zprávu do správce front YORK, lokální správce front tento název vyřeší jako název produktu CLUSQM. Není-li lokální správce front nazván CLUSQM, umístí zprávu do přenosové fronty klastru, která má být přesunuta do CLUSQM. Změní také záhlaví přenosu tak, aby řídíte CLUSQM namísto YORK.

Poznámka: Definice se vztahuje pouze na správce front, který jej provádí. Chcete-li propagovat alias na celý klastr, je třeba přidat atribut CLUSTER do definice vzdálené fronty. Zprávy z jiných správců front, které byly určeny pro produkt YORK , jsou odesílány do produktu CLUSQM.

Změna přenosové fronty nebo určení přenosové fronty při odesílání zpráv

Použití aliasů lze použít k připojení klastru k neklastrového systému. Například správci front v klastru ITALY mohli komunikovat se správcem front s názvem PALERMO, který je mimo klastr. Chcete-li komunikovat, musí jeden z správců front v klastru vystupovat jako brána. Ve správci front brány zadejte příkaz:

```
DEFINE QREMOTE(ROME) RNAME(' ') RQMNAME(PALERMO) XMITQ(X) CLUSTER(ITALY)
```

Příkaz je definice alias správce front. Definuje a inzeruje produkt ROME jako správce front, přes který mohou zprávy z libovolného správce front v klastru ITALY dosáhnout svého cíle na PALERMO. Zprávy vkládané do fronty otevřené s názvem správce front nastaveným na hodnotu ROME jsou odeslány správci front brány s definicí aliasu správce front. Jakmile jsou tyto zprávy vloženy do přenosové fronty X a jsou přesunuty neklastlovými kanály do správce front PALERMO.

Výběr názvu ROME v tomto příkladu není významný. Hodnoty pro QREMOTE a RQMNAME mohou být obě stejné.

Určení místa určení při příjmu zpráv

Když správce front přijme zprávu, extrahuje název cílové fronty a správce front z záhlaví přenosu. Najde definici aliasu správce front se stejným názvem, jako má správce front v záhlaví přenosu. Pokud nalezne jeden, nahradí soubor RQMNAME z definice aliasu správce front pro název správce front v záhlaví přenosu.

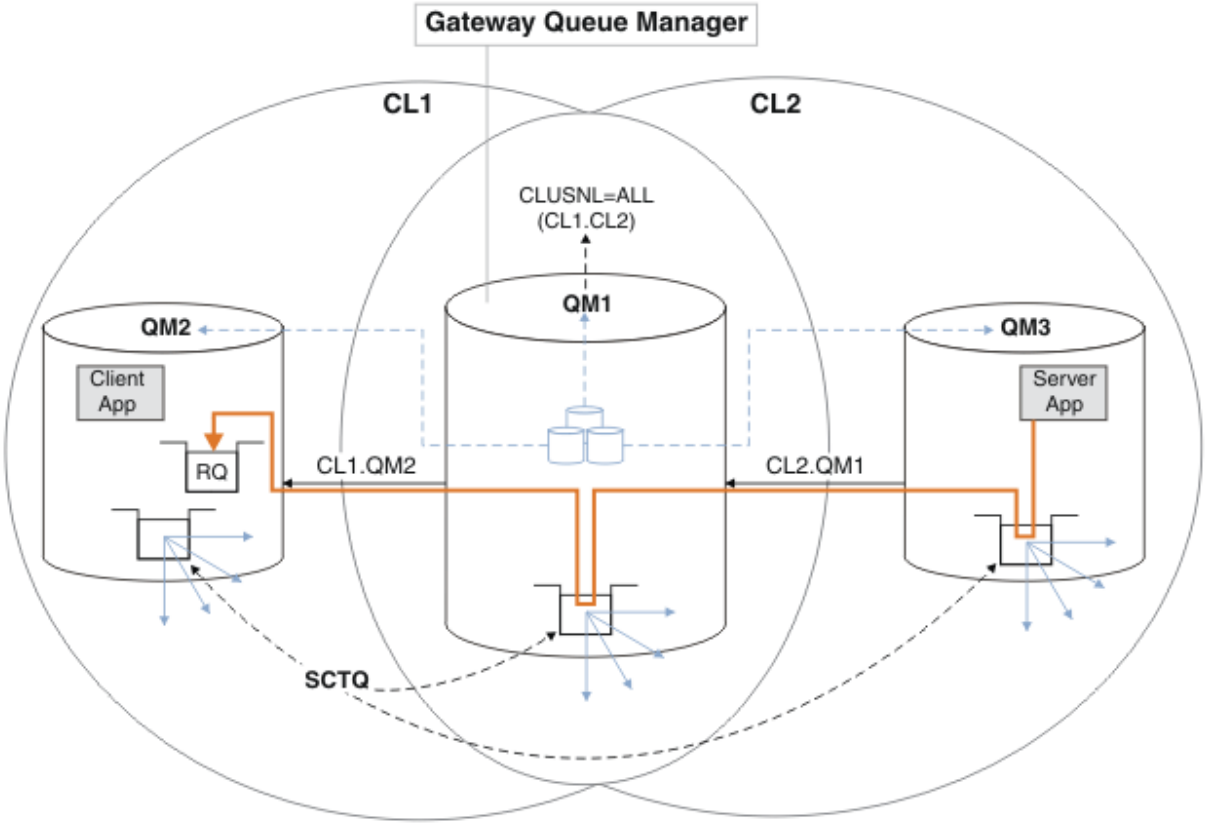
Existují dva důvody pro použití aliasu správce front tímto způsobem:

- Chcete-li směrovat zprávy do jiného správce front
- Chcete-li změnit název správce front tak, aby byl stejný jako lokální správce front, postupujte takto:

Použití aliasů správce front ve správci front brány pro směrování zpráv mezi správci front v různých klastrech.

Aplikace může odeslat zprávu do fronty v jiném klastru pomocí aliasu správce front. Fronta nemusí být frontou klastru. Fronta je definována v jednom klastru. Aplikace je připojena ke správci front v jiném klastru. Správce front brány připojí dva klastry. Není-li fronta definována jako klastrovaná, musí aplikace otevřít frontu za použití názvu fronty a názvu aliasu správce front s klastry. Příklad konfigurace naleznete v části “Vytvoření dvou překrývajících se klastrů se správcem front brány” na stránce 312, ze které se bere tok zpráv s odpovědí znázorněný na obrázku 1.

Diagram zobrazuje cestu, kterou zpráva odpovědi vede zpět do dočasné dynamické fronty s názvem RQ. Serverová aplikace připojená k produktu QM3otevře frontu odpovědí s použitím názvu správce front QM2. Název správce front QM2 je definován jako alias správce front klastru v systému QM1. QM3 směruje zprávu odpovědi na QM1. QM1 směruje zprávu na QM2.



Obrázek 60. Použití aliasu správce front k vrácení zprávy odpovědi do jiného klastru

Způsob, jakým směrování funguje, je následující. Každý správce front v každém klastru má v systému QM1definici aliasu správce front. Aliasy jsou klastrovány ve všech klastrech. Šedé čárkované šipky jednotlivých aliasů pro správce front ukazují, že každý alias správce front je převeden na skutečného správce front alespoň v jednom z klastrů. V tomto případě je alias QM2 klastrován v klastru CL1 i CL2a je interpretován jako skutečný správce front QM2 v souboru CL1. Serverová aplikace vytvoří zprávu odpovědi s použitím názvu fronty pro odpověď RQa názvu správce front pro odpověď QM2. Zpráva je směrována do adresáře QM1 , protože definice aliasu správce front QM2 je definována v systému QM1 v klastru CL2 a správce front QM2 není v klastru CL2. Protože zprávu nelze odeslat do cílového správce front, je odeslána do správce front, který má definici aliasu.

QM1 umístí zprávu do přenosové fronty klastru na QM1 pro přenos do QM2. QM1 směruje zprávu do umístění QM2 , protože definice aliasu správce front v systému QM1 for QM2 definuje QM2 jako skutečného cílového správce front. Definice není kruhová, protože definice aliasů mohou odkazovat pouze na skutečné definice; alias nemůže ukazovat sám na sebe. Skutečnou definici interpretuje QM1, protože jak QM1 , tak QM2 jsou ve stejném klastru CL1. Produkt QM1 zjišťuje informace o připojení pro produkt QM2 z úložiště pro produkt CL1a směruje zprávu do adresáře QM2. Aby

mohla být zpráva přesměrována produktem QM1, musí serverová aplikace otevřít frontu odpovědí s volbou DEFBIND nastavenou na MQBND_BIND_NOT_FIXED. Pokud serverová aplikace otevřela frontu odpovědí s volbou MQBND_BIND_ON_OPEN, zpráva nebude přesměrována a skončí ve frontě nedoručených zpráv.

Použití správce front jako brány v klastru k vyrovnávání pracovní zátěže v důsledku příchodu z mimo klastr.

Definujete frontu s názvem EDINBURGH ve více než jednom správci front v klastru. Chcete, aby klastrový mechanismus vyvažovat pracovní zátěž pro zprávy přicházející do této fronty mimo klastr.

Správce front z prostředí mimo klastr potřebuje pro jednoho správce front v klastru přenosovou frontu a odesílací kanál. Tato fronta se nazývá správce front brány. Chcete-li využít výchozího mechanizmu vyrovnávání pracovní zátěže, je třeba použít jedno z následujících pravidel:

- Správce front brány nesmí obsahovat instanci fronty EDINBURGH .
- Správce front brány určuje CLWLUSEQ(ANY) v systému ALTER QMGR.

Příklad vyvažování pracovní zátěže mimo klastr naleznete v tématu “Konfigurace vyrovnávání pracovní zátěže mimo klastr” na stránce 353 .

Související pojmy

Aliasy fronty pro odpověď a klastry
Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí lze použít s klastry stejně jako v prostředí distribuovaných front.

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
Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry
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 fronty pro odpověď a klastry

Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí lze použít s klastry stejně jako v prostředí distribuovaných front.

Příklad:

- Aplikace ve správci front VENICE odešle zprávu do správce front PISA pomocí volání MQPUT . Aplikace poskytuje v deskriptoru zpráv následující informace o odpovědi na frontu:

```
ReplyToQ='QUEUE'
ReplyToQMgr=''
```

- Aby mohly být odpovědi odeslané do produktu QUEUE přijaty v produktu OTHERQ na PISA, vytvořte definici vzdálené fronty v systému VENICE , která se používá jako alias fronty pro odpověď. Alias je účinný pouze na systému, na kterém byl vytvořen.

```
DEFINE QREMOTE(QUEUE) RNAME(OTHERQ) RQMNAME(PISA)
```

RQMNAME a QREMOTE mohou určovat stejné názvy, a to i v případě, že RQMNAME je sám správcem front klastru.

Související pojmy

Aliasy správce front a klastry
Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy front a klastry
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
Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry
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 správce front a klastry
Aliasy správce front slouží ke skrytí názvu správců front při odesílání zpráv do klastru nebo mimo klastr a pro zprávy o stavu pracovní zátěže odeslané do klastru.

Aliasy fronty pro odpověď a klastry
Definice alias fronty pro odpověď se používá k určení alternativních názvů pro informace o odpovědi. Definice alias fronty odpovědí lze použít s klastry stejně jako v prostředí distribuovaných front.

Související úlohy

Konfigurace požadavku/odpovědi na klastr
Konfigurujte cestu ke zprávám požadavku/odpovědi ze správce front mimo klastr. Skryjte vnitřní podrobnosti klastru pomocí správce front brány jako komunikační cesty do klastru a z něj.

Konfigurace požadavku/odpovědi z klastru
Konfigurujte cestu ke zprávě s požadavkem/odpovědí z klastru do správce front mimo klastr. Skrytí podrobností o tom, jak správce front v klastru komunikuje mimo klastr pomocí správce front brány.

Konfigurace vyrovnávání pracovní zátěže mimo klastr
Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Konfigurace cest zpráv mezi klastry
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 šířit práci obsluhy fronty na více serverech. Existuje několik faktorů, které mohou zabránit opětnému zařazení zpráv do jiného správce front v případě selhání.

Kromě nastavení klastrů za účelem snížení administrace systému můžete vytvořit klastry, ve kterých bude více než jeden správce front hostitelem instance stejné fronty.

Můžete uspořádat klastr tak, aby byli správci front v sobě klony. Každý správce front je schopen spouštět stejné aplikace a mít lokální definice stejných front. z/OS Příklad: V paralelním prostředí sysplex produktu z/OS mohou klonované aplikace přistupovat k datům ve sdílené databázi Db2 nebo v databázi VSAM (Virtual Storage Access Method). Pracovní zátěž mezi správci front můžete rozložit tak, že budete mít několik instancí určité aplikace. Každá instance aplikace přijímá zprávy a spouští se nezávisle na ostatních.

Výhody použití klastrů tímto způsobem jsou následující:

- Zvýšená dostupnost front a aplikací.
- Rychlejší propustnost zpráv.
- Více rozložení pracovní zátěže ve vaší síti.

Každý správce front, který je hostitelem instance určité fronty, může zpracovávat zprávy určené pro danou frontu a aplikace nepojmenují správce front při odesílání zpráv. Pokud klastr obsahuje více než jednu instanci stejné fronty, produkt IBM MQ vybere správce front, do kterého má být směrována zpráva. Vhodné cíle jsou zvoleny na základě dostupnosti správce front a fronty a na určitém počtu atributů specifických pro pracovní zátěž klastru, které jsou přidruženy ke správcům front, frontám a kanálům. Viz Vyrovnávání pracovní zátěže v klastrech.

z/OS V produktu IBM MQ for z/OSmohou správci front, kteří jsou ve skupinách sdílení front, hostit fronty klastru jako sdílené fronty. Sdílené fronty klastru jsou k dispozici pro všechny správce front ve stejné skupině sdílení front. For example, in Klastr s více instancemi stejné fronty., either or both of the

queue managers QM2 and QM4 can be a shared-queue manager. Každý má definici pro frontu Q3. Kterýkoli z správců front ve stejné skupině sdílení front jako produkt QM4 může číst zprávu vkládanou do sdílené fronty Q3. Každá skupina sdílení front může obsahovat až 32 správců front, přičemž každý z nich má přístup ke stejným datům. Sdílení front významně zvyšuje propustnost vašich zpráv.

Další informace o konfiguracích klastru pro správu pracovní zátěže naleznete v následujících dílčích tématech:

Související pojmy

Porovnání klastrování a distribuovaných front

Distribuované fronty a klastry

Komponenty klastru

Kanály klastru

Co se stane, pokud je fronta klastru zakázána pro MQPUT

“Směrování zpráv do a z klastrů” na stránce 344
Aliasy fronty, aliasy správců front a definice vzdálených front slouží k připojení klastrů k externím správcům front a dalším klastrům.

Související úlohy

Zápis a kompilace uživatelských procedur pracovní zátěže klastru

“Konfigurace klastru správce front” na stránce 265
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 277
Postupujte podle těchto pokynů, chcete-li nastavit příklad klastru. Samostatné pokyny popisují nastavení klastru na TCP/IP, LU 6.2a s jednou přenosovou frontou nebo více přenosových front. Otestujte činnost klastru odesláním zprávy z jednoho správce front do druhého.

“Konfigurace vyrovnávání pracovní zátěže mimo klastr” na stránce 353
Konfigurujte cestu ke zprávám ze správce front mimo klastr do libovolné kopie fronty klastru. Výsledkem je požadavek na vyvážení pracovní zátěže z mimo klastr na každou instanci fronty klastru.

Související odkazy

Vyrovnávání pracovní zátěže nastavené na odesílacím kanálu klastru nefunguje.

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 na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

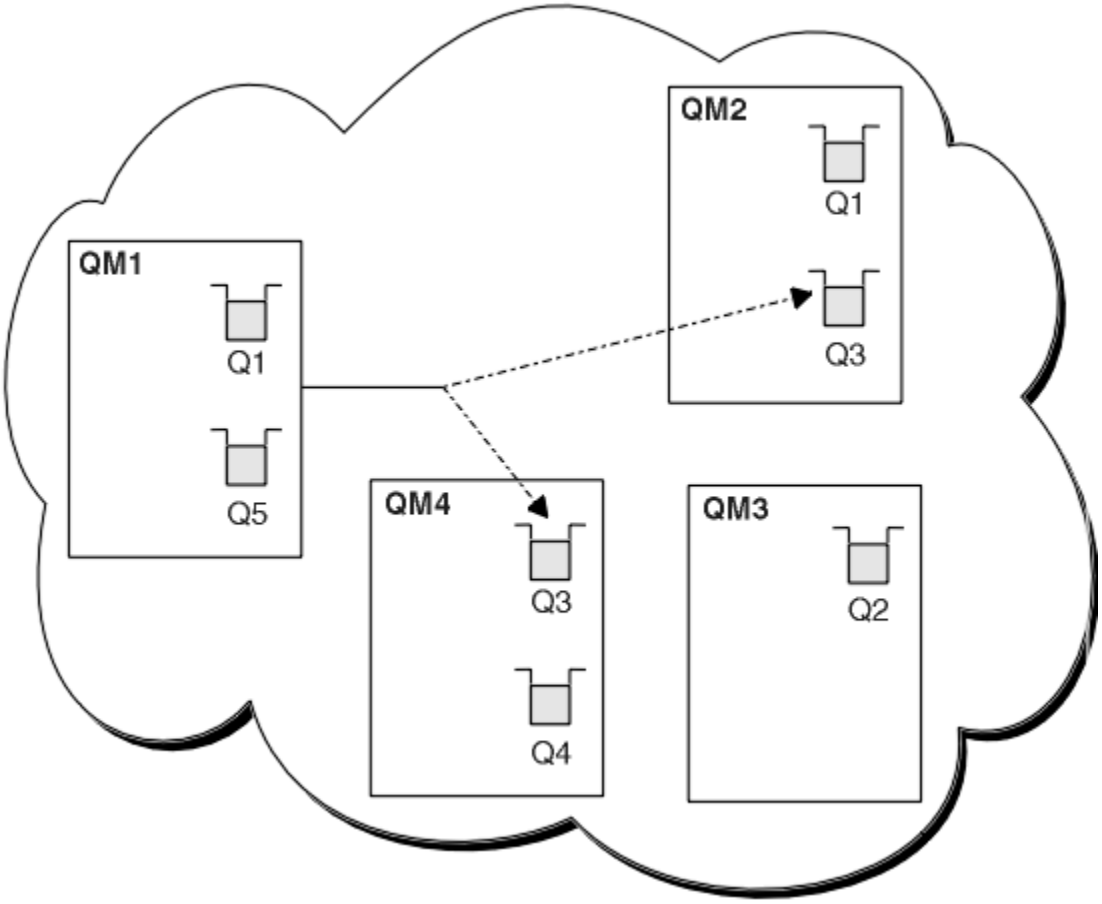
Obrázek 61 na stránce 364 ukazuje klastr, v němž je pro frontu Q3více než jedna definice. Pokud aplikace v produktu QM1 vloží zprávu do produktu Q3, nemusí nutně vědět, která instance produktu Q3 bude zpracovávat svou zprávu. Je-li aplikace spuštěna na serveru QM2 nebo v produktu QM4, , kde jsou lokální instance produktu Q3, je lokální instance produktu Q3 standardně otevřena. Nastavením atributu fronty CLWLUSEQ lze lokální instanci fronty považovat stejně jako vzdálenou instanci fronty.

Volba MQOPEN DefBind řídí, zda je cílový správce front vybrán při vyvolání volání MQOPEN , nebo když je zpráva přenesena z přenosové fronty.

Nastavíte-li volbu DefBind na hodnotu MQBND_BIND_NOT_FIXED , lze zprávu odeslat na instanci fronty, která je k dispozici při přenosu zprávy. Tím se vyvarujete následujících problémů:

- Pokud zpráva dorazí do cílového správce front, není cílová fronta k dispozici.
- Stav fronty se změnil.
- Zpráva byla vložena pomocí aliasu fronty klastru a ve správci front neexistuje žádná instance cílové fronty, ve které je definována instance aliasu fronty klastru.

Jsou-li tyto problémy zjištěny v čase přenosu, je požadována jiná dostupná instance cílové fronty a zpráva je přesměrována. Nejsou-li k dispozici žádné instance fronty, bude zpráva umístěna do fronty nedoručených zpráv.



Obrázek 61. Klastr s více instancemi stejné fronty.

Jedním z faktorů, které mohou zabránit přesměrování zpráv, je, že zprávy byly přiřazeny k opravenému správci front nebo kanálu s volbou `MQBND_BIND_ON_OPEN`. Zprávy, které jsou svázány s produktem `MQOPEN` , nejsou nikdy znovu přiděleny jinému kanálu. Všimněte si také, že k opětovnému přidělení zpráv dochází pouze tehdy, když se kanál klastru skutečně nedaří. K opětovné alokaci nedojde v případě, že kanál již selhal.

Systém se pokusí přesměrovat zprávu v případě, že správce cílových front přestane pracovat. Tímto způsobem neovlivní integritu zprávy tím, že se spustí riziko ztráty nebo vytvoření duplikátu. Pokud správce front selže a zanechá zprávu v nejistém stavu, tato zpráva není přesměrována.

z/OS V systému IBM MQ for z/OSnedojde k úplnému zastavení kanálu, dokud nedojde k dokončení procesu nového přidělení zprávy. Zastavení kanálu s režimem nastaveným na hodnotu `FORCE` nebo `TERMINATE` přeruší proces, takže pokud tak učiníte, mohou být některé zprávy `BIND_NOT_FIXED` již přerozděleny do jiného kanálu nebo mohou být zprávy mimo pořadí.

Poznámka: z/OS

1. Před nastavením klastru, který má více instancí stejné fronty, zajistěte, aby vaše zprávy neměly závislosti na sobě navzájem. Například je třeba, aby byly zpracovány v určité posloupnosti nebo ve stejném správci front.
2. Učinit definice pro různé instance stejné fronty identické. Jinak získáte odlišné výsledky z různých volání `MQINQ` .

Související pojmy

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru
Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů
Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu Přidání nového správce front do klastru. Obsahuje tři správce front; produkty LONDON a NEWYORK obsahují úplná úložiště, produkt PARIS uchovává dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK . Aplikace je řízena doručením zpráv ve frontě INVENTQ .
- Chceme přidat instanci produktu INVENTQ , která poskytuje dodatečnou kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Informace o této úloze

Chcete-li přidat správce front, který je hostitelem fronty lokálně, postupujte podle následujících kroků.

Postup

1. Změňte správce front produktu PARIS .

   Aby aplikace v Paříži používala INVENTQ v Paříži a v New Yorku, musíme o tom informovat správce front. V systému PARIS zadejte následující příkaz:

   ```
   ALTER QMGR CLWLUSEQ(ANY)
   ```
2. Přezkoumejte aplikaci soupisu pro afinity zpráv.

Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv. Další informace najdete v tématu Práce s spřízněnostmi zpráv.

3. Instalovat inventární aplikaci na systém v Paříži.
4. Definujte frontu klastru INVENTQ.

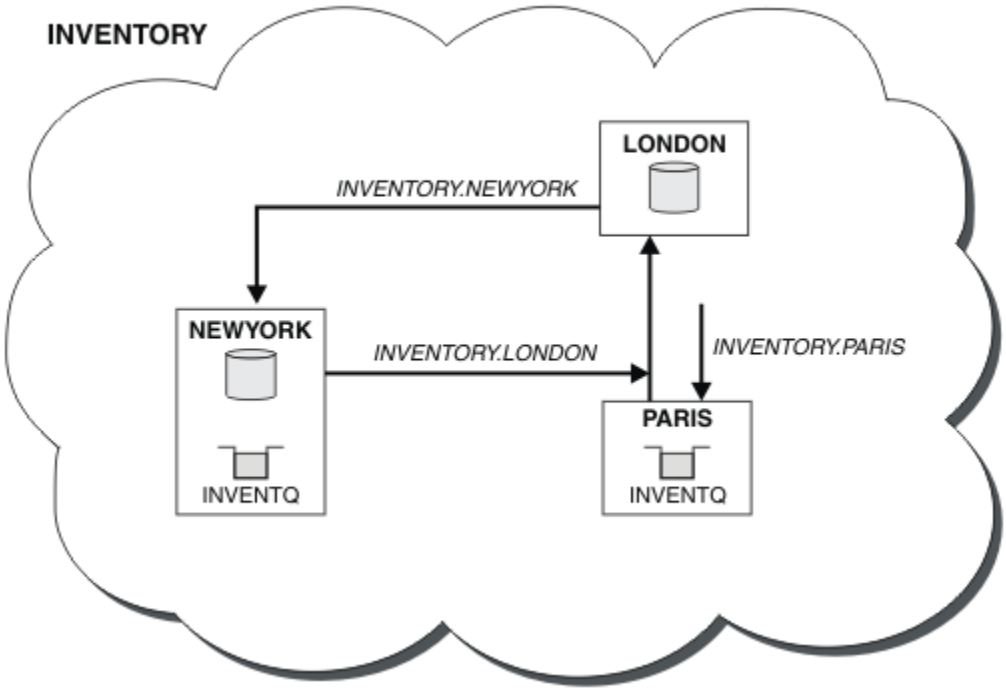
   Frontu INVENTQ , která je již hostována správcem front NEWYORK , je také hostována pomocí PARIS. Definujte jej ve správci front produktu PARIS takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak dosud neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front PARIS. Listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 62 na stránce 366 zobrazuje klastr nastavený touto úlohou.



Obrázek 62. Klastr INVENTORY se třemi správci front

Úpravy tohoto klastru byly provedeny bez změny správců front NEWYORK nebo LONDON. Úplná úložiště v těchto správcích front jsou aktualizována automaticky s informacemi, které potřebují k odesílání zpráv do produktu INVENTQ na adrese PARIS.

Jak pokračovat dále

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správcích front v klastru. To zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje distribuci pracovní zátěže mezi dvěma správci front. Zprávy ukládané do INVENTQ některým ze správců front LONDON, NEWYORK, PARIS jsou směrovány střídavě na PARIS nebo NEWYORK, takže pracovní zátěž je vyvážená.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry
Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Použití dvou sítí v klastru
Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů
Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu "Přidání správce front do klastru". Obsahuje tři správce front; produkty LONDON a NEWYORK obsahují úplná úložiště, produkt PARIS uchovává dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK . Aplikace je řízena doručením zpráv ve frontě INVENTQ .
- Do produktu TOKYO se přidává nové úložiště, kde jsou dvě různé sítě. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Informace o této úloze

Chcete-li používat dvě sítě v klastru, postupujte takto.

Postup

1. Rozhodněte se, které úplné úložiště TOKYO odkazuje na první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Staví své vlastní dílčí úložiště. To není zvláštní význam, který úložiště si vyberete. V tomto příkladě je vybrána volba NEWYORK . Poté, co se nový správce front připojil ke klastru, komunikuje s oběma úložišti.
2. Definujte kanály CLUSRCVR .

   Každý správce front v klastru musí definovat příjemce klastru, na kterém může přijímat zprávy. Tento správce front musí být schopen komunikovat na každé síti.

```
DEFINE CHANNEL(INVENTORY.TOKYO.NETB) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME('TOKYO.NETB.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
channel using network B for TOKYO')

DEFINE CHANNEL(INVENTORY.TOKYO.NETA) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
CONNAME('TOKYO.NETA.CMSTORE.COM') CLUSTER(INVENTORY) DESCR('Cluster-receiver
channel using network A for TOKYO')
```

3. Definujte kanál CLUSSDR ve správci front TOKYO.

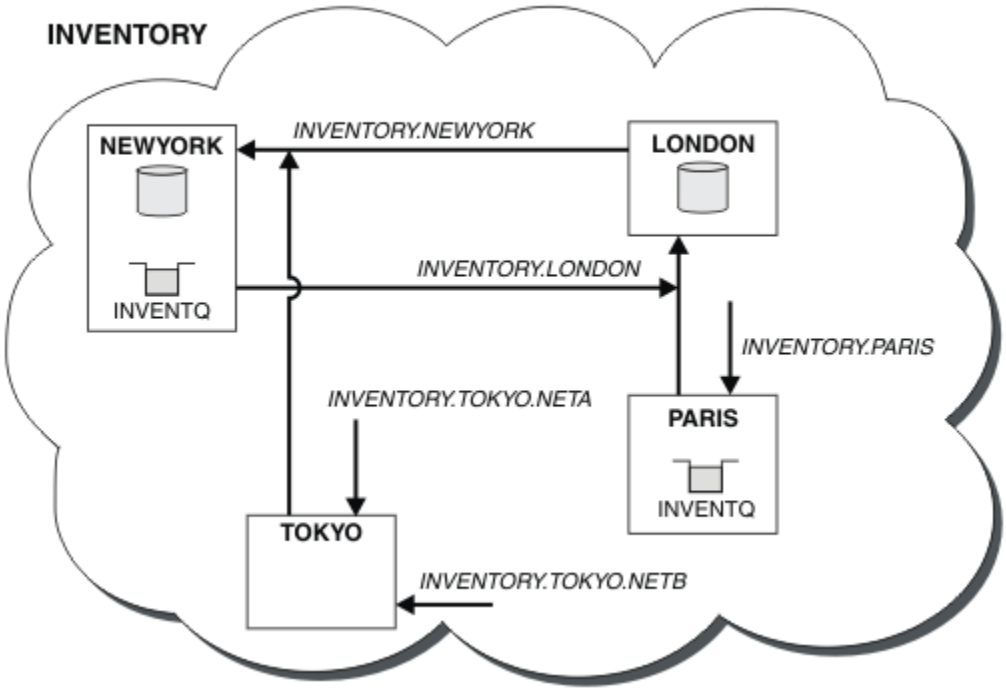
   Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK, takže TOKYO potřebuje následující definici:

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-sender
   channel from TOKYO to repository at NEWYORK')
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front PARIS. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 63 na stránce 368 zobrazuje klastr nastavený touto úlohou.



Obrázek 63. Klastr INVENTORY se čtyřmi správci front

Při vytváření pouze tří definic jsme přidali správce front TOKYO do klastru se dvěma různými dostupnými přenosovými cestami k síti.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry
Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů
Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

"Přidání správce front do klastru" na stránce 288
Chcete-li přidat správce front do vytvořeného klastru, postupujte podle následujících pokynů. Zprávy na fronty klastru a témata se přenášejí pomocí jedné přenosové fronty klastru SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu "Použití dvou sítí v klastru" na stránce 367. Obsahuje čtyři správce front; LONDON a NEWYORK drží úplná úložiště; PARIS a TOKYO uchovávají dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front NEWYORK. Správce front produktu TOKYO má dvě různé sítě, na kterých může komunikovat.
- Chcete vytvořit jednu ze sítí na primární síti a jinou síť ze záložní sítě. Máte v plánu použít záložní síť, pokud existuje problém s primární sítí.

Informace o této úloze

Atribut NETPRTY použijte ke konfiguraci primární a sekundární sítě v klastru.

Postup

Změňte existující kanály CLUSRCVR na systému TOKYO.

Chcete-li označit, že kanál je primární kanál a kanál B kanál je sekundární kanál, použijte následující příkazy:

a) `ALTER CHANNEL(INVENTORY.TOKYO.NETA) CHLTYPE(CLUSRCVR) NETPRTY(2) DESCR('Main cluster-receiver channel for TOKYO')`

b) `ALTER CHANNEL(INVENTORY.TOKYO.NETB) CHLTYPE(CLUSRCVR) NETPRTY(1) DESCR('Backup cluster-receiver channel for TOKYO')`

Jak pokračovat dále

Konfigurací kanálu s různými prioritami sítě jste nyní definovali klastr, který má primární síť a sekundární síť. Správci front v klastru, kteří používají tyto kanály, automaticky používají primární síť, pokud jsou k dispozici. Pokud primární síť není k dispozici, správci front se v případě, že nejsou k dispozici primární sítě, mohou používat sekundární sítě.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně

Postupujte podle těchto pokynů, chcete-li přidat instanci portálu `INVENTQ` , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru

Chcete-li přidat nové úložiště v produktu `TOKYO` , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Přidání fronty jako zálohy

Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr `INVENTORY` byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 288. Obsahuje tři správce front; produkty `LONDON` a `NEWYORK` obsahují úplná úložiště, produkt `PARIS` uchovává dílčí úložiště. Aplikace inventáře je spuštěna na systému v New Yorku, který je připojen ke správci front `NEWYORK` . Aplikace je řízena doručením zpráv ve frontě `INVENTQ` .

- Probíhá vytváření nového úložiště v Chicagu za účelem poskytnutí zálohy pro systém inventáře, který se nyní spouští v New Yorku. Chicagský systém se používá pouze v případě, že je problém s New Yorkem.

Informace o této úloze

Chcete-li přidat frontu, která bude sloužit jako záloha, postupujte takto.

Postup

1. Rozhodněte se, které úplné úložiště CHICAGO odkazuje na první.

   Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Staví své vlastní dílčí úložiště. Nemá zvláštní význam, které úložiště si vyberete pro konkrétního správce front. V tomto příkladě je vybrána volba NEWYORK . Poté, co se nový správce front připojil ke klastru, komunikuje s oběma úložišti.
2. Definujte kanál CLUSRCVR .

   Každý správce front v klastru musí definovat příjemce klastru, na kterém může přijímat zprávy. V systému CHICAGOdefinujte:

   ```
   DEFINE CHANNEL(INVENTORY.CHICAGO) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(CHICAGO.CMSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-receiver
   channel for CHICAGO')
   ```
3. Definujte kanál CLUSSDR ve správci front CHICAGO.

   Každý správce front v klastru musí definovat jeden odesílací kanál klastru, na kterém může odesílat zprávy do svého prvního úplného úložiště. V tomto případě jsme zvolili NEWYORK, takže CHICAGO potřebuje následující definici:

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY) DESCR('Cluster-sender
   channel from CHICAGO to repository at NEWYORK')
   ```
4. Změňte existující frontu klastru INVENTQ.

   Hlavní instancí fronty je produkt INVENTQ , který je již hostitelem správce front NEWYORK .

   ```
   ALTER QLOCAL(INVENTQ) CLWLPRTY(2)
   ```
5. Přezkoumejte aplikaci soupisu pro afinity zpráv.

   Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv.
6. Nainstalujte inventární aplikaci na systém v produktu CHICAGO.
7. Definujte záložní frontu klastru INVENTQ

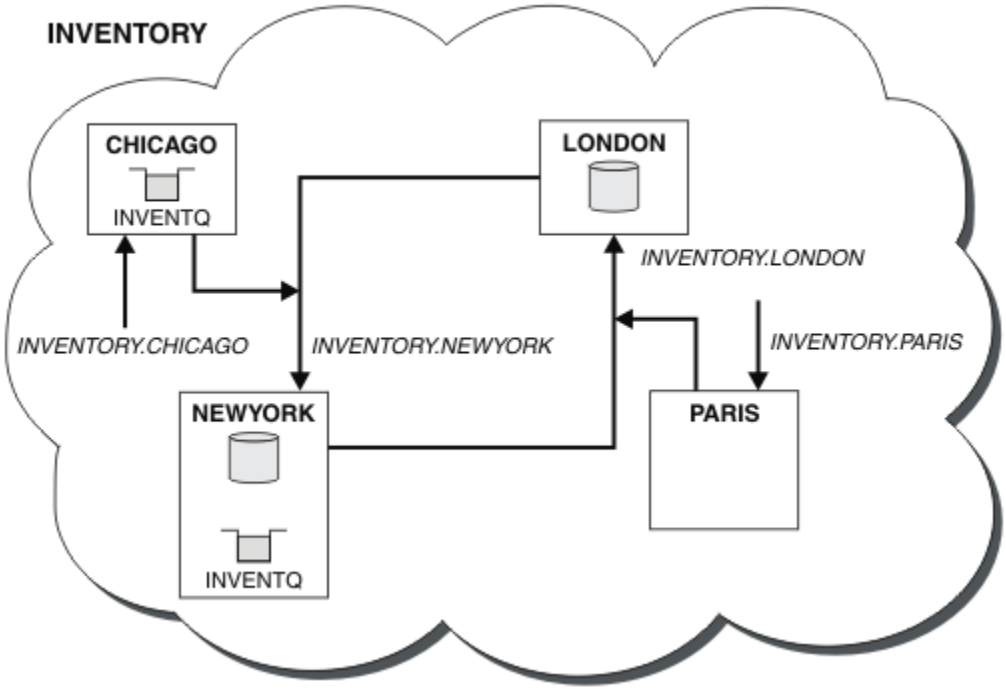
   Server INVENTQ , který je již hostován správcem front NEWYORK , je také hostován jako záloha pomocí CHICAGO. Definujte jej ve správci front produktu CHICAGO takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY) CLWLPRTY(1)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front CHICAGO. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 64 na stránce 372 zobrazuje klastr nastavený touto úlohou.



Obrázek 64. Klastr INVENTORY se čtyřmi správci front

Fronta produktu INVENTQ a inventární aplikace jsou nyní hostovány na dvou správcích front v klastru. Správce front produktu CHICAGO je zálohou. Zprávy odeslané do INVENTQ jsou směrovány na NEWYORK , pokud nejsou k dispozici, když jsou odeslány do CHICAGO.

Poznámka:

Dostupnost vzdáleného správce front je založena na stavu kanálu s daným správcem front. Když se kanály spustí, jejich stav se změní několikrát, přičemž některé stavy jsou méně vhodnější než algoritmus správy pracovní zátěže klastru. V praxi to znamená, že lze zvolit nižší prioritu (záložní) místa určení, zatímco se spouští kanály pro vyšší prioritu (primární) cíle.

Potřebujete-li zajistit, aby žádné zprávy nepřešli na místo určení zálohování, nepoužívejte CLWLPRTY. Zvažte použití samostatných front nebo příkazu CLWLRANK s ručním přepnutím z primární databáze na záložní server.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry
Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru
Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Omezení počtu používaných kanálů
Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Omezení počtu používaných kanálů

Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Aplikace pro kontrolu cen musí být nainstalována na různých správcích front. Počet kanálů, které jsou používány k nízkému počtu kanálů, je omezeno tím, že je omezen počet aktivních kanálů každého serveru. Aplikace je řízena doručením zpráv ve frontě PRICEQ .
- Čtyři správci front serveru hostí aplikaci kontroly cen. Dva správci front dotazů odesílají zprávy do produktu PRICEQ za účelem zadání dotazu na cenu. Dva další správci front jsou konfigurováni jako úplná úložiště.

Informace o této úloze

Chcete-li omezit počet použitých kanálů, postupujte takto.

Postup

1. Vyberte dvě úplná úložiště.

   Zvolte dva správce front, kteří budou úplnými úložišti pro váš klastr kontroly cen. Nazývaly se REPOS1 a REPOS2.

   Spusťte následující příkaz:

   ```
   ALTER QMGR REPOS(PRICECHECK)
   ```
2. Definujte kanál CLUSRCVR pro každého správce front.

   V každém správci front v klastru definujte kanál příjemce klastru a odesílací kanál klastru. Nezáleží na tom, která definice je definována jako první.

   ```
   DEFINE CHANNEL(PRICECHECK.SERVE1) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(SERVER1.COM) CLUSTER(PRICECHECK) DESCR('Cluster-receiver channel')
   ```
3. Definujte kanál CLUSSDR pro každého správce front.

   Vytvořte v každém správci front definici CLUSSDR a propojte tohoto správce front s jedním nebo více správci front úplného úložiště.

   ```
   DEFINE CHANNEL(PRICECHECK.REPOS1) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(REPOS1.COM) CLUSTER(PRICECHECK) DESCR('Cluster-sender channel to
   repository queue manager')
   ```
4. Nainstalujte aplikaci kontroly cen.
5. Definujte frontu PRICEQ ve všech správcích front serveru.

Vydejte následující příkaz pro každý z nich:

```
DEFINE QLOCAL(PRICEQ) CLUSTER(PRICECHECK)
```

6. Omezit počet kanálů používaných dotazy

   Na správcích front dotazů omezujeme počet používaných aktivních kanálů, a to zadáním následujících příkazů pro každou z těchto možností:

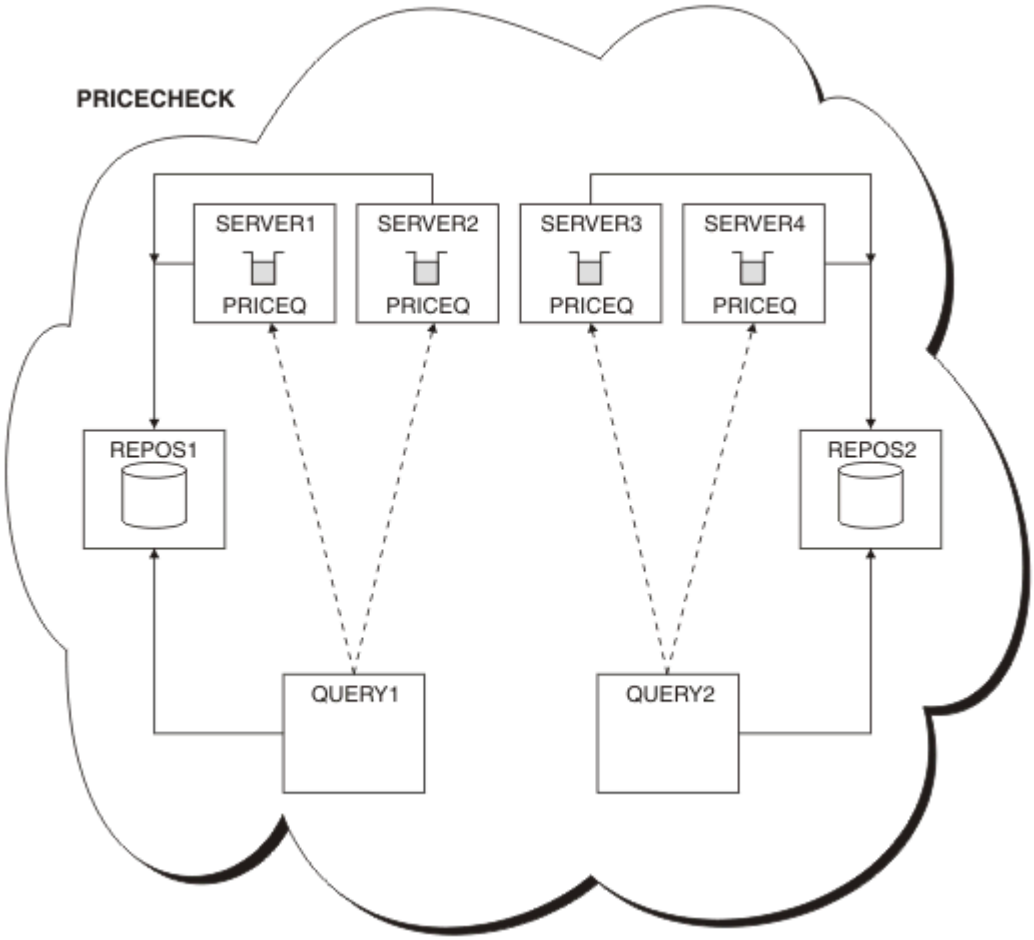
   ```
   ALTER QMGR CLWLMRUC(2)
   ```

7. Pokud jste tak dosud neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener.

   Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

Obrázek 65 na stránce 374 zobrazuje klastr nastavený touto úlohou.



Obrázek 65. Klastr PRICECHECK se čtyřmi správci front serveru, dvěma úložišti a dvěma správci front dotazů.

Ačkoli jsou v klastru PRICECHECK k dispozici čtyři instance fronty produktu PRICEQ , každý dotazovací správce front používá pouze dva dva z nich. Správce front produktu QUERY1 má například pouze aktivní kanály pro správce front SERVER1 a SERVER2 . Pokud se produkt SERVER1 stane nedostupným, správce front produktu QUERY1 by pak mohl začít používat jiného správce front, například SERVER3.

Související pojmy

Příklad klastru s více než jednou instancí fronty

V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry
Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru
Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru
Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Přidání výkonnějšího správce front, který je hostitelem fronty

Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Než začnete

Poznámka: Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 288. Obsahuje tři správce front: LONDON a NEWYORK udržují úplná úložiště, PARIS ukládá dílčí úložiště a umisťuje zprávy z produktu INVENTQ. Aplikace soupisu se spustí na systému v New Yorku připojeném ke správci front NEWYORK . Aplikace je řízena doručením zpráv ve frontě INVENTQ .
- V Los Angeles je vytvářený nový obchod. Chcete-li poskytnout dodatečnou kapacitu, chcete spustit systém inventářů v Los Angeles stejně jako New York. Nový správce front může zpracovat dvakrát tolik zpráv jako New York.

Informace o této úloze

Chcete-li přidat výkonnějšího správce front, který je hostitelem fronty, postupujte podle následujících kroků.

Postup

1. Rozhodněte se, které úplné úložiště LOSANGELES odkazuje na první.

2. Každý správce front v klastru musí odkazovat na jedno nebo druhé z úplných úložišť, aby mohl shromažďovat informace o klastru. Staví své vlastní dílčí úložiště. To není zvláštní význam, který úložiště si vyberete. V tomto příkladě je vybrána volba NEWYORK . Poté, co se nový správce front připojil ke klastru, komunikuje s oběma úložišti.

   ```
   DEFINE CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSSDR) TRPTYPE(TCP)
   CONNAME(NEWYORK.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-sender channel from LOSANGELES to repository at NEWYORK')
   ```

3. Definujte kanál CLUSRCVR ve správci front LOSANGELES.

   Každý správce front v klastru musí definovat kanál příjemce klastru, ve kterém může přijímat zprávy. V systému LOSANGELESdefinujte:

   ```
   DEFINE CHANNEL(INVENTORY.LOSANGELES) CHLTYPE(CLUSRCVR) TRPTYPE(TCP)
   CONNAME(LOSANGELES.CHSTORE.COM) CLUSTER(INVENTORY)
   DESCR('Cluster-receiver channel for queue manager LOSANGELES')
   CLWLWGHT(2)
   ```

   Přijímací kanál klastru oznamuje dostupnost zpráv od jiných správců front v klastru INVENTORY. Nastavení CLWLWGHT na dva zajistí, že správce front v Los Angeles dostane dvakrát tolik zpráv o inventuře jako New York (je-li kanál pro NEWYORK nastaven na hodnotu jedna).

4. Upravte kanál CLUSRCVR ve správci front NEWYORK.

   Ujistěte se, že správce front v Los Angeles dostane dvakrát tolik inventárních zpráv jako New York. Upravte definici přijímacího kanálu klastru.

   ```
   ALTER CHANNEL(INVENTORY.NEWYORK) CHLTYPE(CLUSRCVR) CLWLWGHT(1)
   ```

5. Přezkoumejte aplikaci soupisu pro afinity zpráv.

   Než budete pokračovat, ujistěte se, že aplikace zásob nemá žádné závislosti na pořadí zpracování zpráv.

6. Instalovat inventární aplikaci na systém v Los Angeles
7. Definujte frontu klastru INVENTQ.

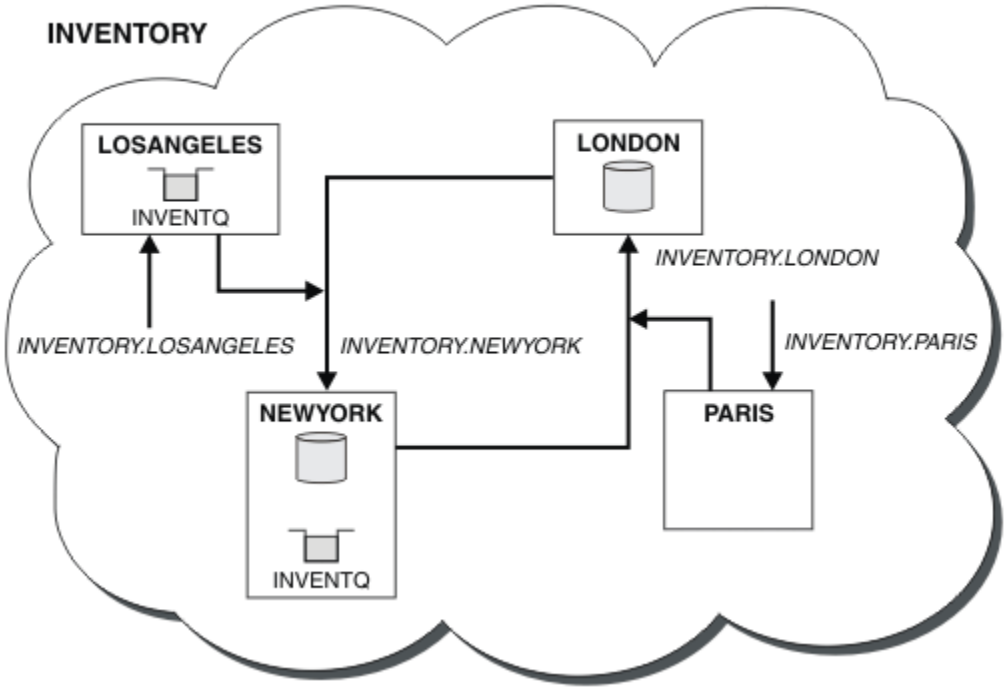
   Frontu INVENTQ , která je již hostována správcem front NEWYORK , je také hostována pomocí LOSANGELES. Definujte jej ve správci front produktu LOSANGELES takto:

   ```
   DEFINE QLOCAL(INVENTQ) CLUSTER(INVENTORY)
   ```

   Nyní, když jste dokončili všechny definice, pokud jste tak již neučinili, spusťte inicializátor kanálu na serveru IBM MQ for z/OS. Na všech platformách spusťte program modulu listener na správci front LOSANGELES. Program modulu listener naslouchá příchozím požadavkům sítě a spouští kanál příjemce klastru, je-li potřeba.

Výsledky

“Přidání výkonnějšího správce front, který je hostitelem fronty” na stránce 375 zobrazuje klastr nastavený touto úlohou.



Obrázek 66. Klastr INVENTORY se čtyřmi správci front

Tato úprava klastru byla dokončena, aniž byste museli měnit správce front LONDON a PARIS. Úložiště v těchto správcích front jsou automaticky aktualizována informacemi, které potřebují k odesílání zpráv do produktu INVENTQ na adrese LOSANGELES.

Jak pokračovat dále

Fronta produktu INVENTQ a katalogizace jsou hostovány na dvou správcích front v klastru. Konfigurace zvyšuje jejich dostupnost, urychluje propustnost zpráv a umožňuje distribuci pracovní zátěže mezi dvěma správci front. Zprávy, které byly do produktu INVENTQ vloženy buď pomocí produktu LOSANGELES , nebo NEWYORK , jsou zpracovávány instancí v lokálním správci front, kdykoli je to možné. Zprávy zařazené do LONDON nebo PARIS jsou směrovány na LOSANGELES nebo NEWYORK, dvakrát tolik zpráv, které se posílají na LOSANGELES.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Programování aplikací a klastry
Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci portálu INVENTQ , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru
Chcete-li přidat nové úložiště v produktu TOKYO , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů
Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Programování aplikací a klastry

Nemusíte provádět žádné změny v programování, abyste mohli využívat více instancí stejné fronty. Některé programy však nebudou pracovat správně, pokud se posloupnosti zpráv neodešle do stejné instance fronty.

Aplikace mohou otevřít frontu pomocí volání `MQOPEN` . Aplikace používají volání `MQPUT` k vložení zpráv do otevřené fronty. Aplikace mohou vložit jednu zprávu do fronty, která ještě není otevřená, pomocí volání `MQPUT1` .

Pokud jste nastavili klastry, které mají více instancí stejné fronty, neexistují žádné specifické pokyny pro programování aplikací. Chcete-li však využívat výhody správy pracovní zátěže pro klastrování, může být zapotřebí upravit vaše aplikace. Pokud jste nastavili síť, ve které existuje více definic stejné fronty, přezkoumejte své aplikace pro zprávy s afinitními zprávami.

Předpokládejme například, že máte dvě aplikace, které se spoléhají na posloupnost zpráv, které mezi nimi proudí ve formě otázek a odpovědí. Pravděpodobně budete chtít odpovědi vrátit se zpět na stejného správce front, který odeslal otázku. Je důležité, aby rutina správy pracovní zátěže neodeslala žádné zprávy do žádného správce front, který je hostitelem kopie fronty odpovědí.

Můžete mít aplikace, které vyžadují zpracování zpráv v posloupnosti (například aplikace replikace databáze, která odesílá dávky zpráv, které musí být načteny v posloupnosti). Použití segmentovaných zpráv může také způsobit problém afinity.

Otevření lokální nebo vzdálené verze cílové fronty

Uvědomte si, jak správce front zvolí, zda má být použita lokální nebo vzdálená verze cílové fronty.

1. Správce front otevře lokální verzi cílové fronty pro čtení zpráv nebo pro nastavení atributů fronty.
2. Správce front otevře jakoukoli instanci cílové fronty pro zápis zpráv, je-li splněna alespoň jedna z následujících podmínek:
   - Lokální verze cílové fronty neexistuje.
   - Správce front uvádí `CLWLUSEQ(ANY)` v systému `ALTER QMGR`.
   - Fronta ve správci front uvádí `CLWLUSEQ(ANY)`.

Související pojmy

Příklad klastru s více než jednou instancí fronty
V tomto příkladu klastru s více než jednou instancí fronty jsou zprávy směrovány na různé instance fronty. Zprávu můžete vynutit u konkrétní instance fronty a můžete zvolit odeslání posloupnosti zpráv jednomu z správců front.

Související úlohy

Přidání správce front, který je hostitelem fronty lokálně
Postupujte podle těchto pokynů, chcete-li přidat instanci portálu `INVENTQ` , abyste poskytli další kapacitu pro spuštění systému aplikace zásob v Paříži a New Yorku.

Použití dvou sítí v klastru
Chcete-li přidat nové úložiště v produktu `TOKYO` , kde jsou dvě různé sítě, postupujte podle těchto pokynů. Obojí musí být k dispozici pro komunikaci se správcem front v Tokiu.

Použití primární a sekundární sítě v klastru

Postupujte podle těchto pokynů, chcete-li vytvořit jednu síť primární sítě a další síť ze záložní sítě. Použijte záložní síť, pokud se vyskytl problém s primární sítí.

Přidání fronty jako zálohy
Postupujte podle těchto pokynů, chcete-li poskytnout zálohu v Chicagu pro systém soupisu, který je nyní spuštěn v New Yorku. Systém Chicaga se používá pouze v případě, že se jedná o problém s newyorským systémem.

Omezení počtu používaných kanálů
Postupujte podle těchto pokynů, chcete-li omezit počet aktivních kanálů, které každý server spustí, je-li na různých správcích front nainstalována aplikace kontroly cen.

Přidání výkonnějšího správce front, který je hostitelem fronty
Postupujte podle těchto pokynů, chcete-li poskytnout dodatečnou kapacitu spuštěním systému soupisu v Los Angeles stejně jako New York, kde Los Angeles dokáže zvládnout dvojnásobek počtu zpráv jako New York.

Práce s afinitními zprávami
Afinity zpráv jsou zřídka součástí dobrého návrhu programování. Chcete-li plně využívat klastrování, je třeba odstranit afinity zprávy. Pokud nemůžete odebrat afinity zpráv, můžete vynutit doručení souvisejících zpráv pomocí stejného kanálu a stejného správce front.

Máte-li aplikace se spřízněnostmi zpráv, odeberte před spuštěním použití klastrů afinity.

Odebrání afinit zpráv zvyšuje dostupnost aplikací. Aplikace odešle dávku zpráv s afinními ke správci front. Správce front selže po přijetí pouze části dávky. Odesílající správce front musí před odesláním dalších zpráv čekat na zotavení a zpracování nedokončené dávky zpráv.

Odebrání afinit zpráv zlepšuje také rozšiřitelnost aplikací. Dávkové zpracování zpráv s afinními může zamknout prostředky v cílovém správci front během čekání na následné zprávy. Tyto prostředky mohou zůstat zamčené po dlouhou dobu, čímž brání ostatním aplikacím ve své práci.

Kromě toho afinity zpráv brání tomu, aby rutiny správy pracovní zátěže klastru mohly provádět nejlepší volbu správce front.

Chcete-li odstranit afinity, zvažte následující možnosti:

- Přenášení informací o stavu ve zprávách
- Udržování informací o stavu v nestabilním úložišti přístupném pro libovolného správce front, například v databázi Db2
- Replikace dat jen pro čtení tak, aby byla přístupná více než jednomu správci front

Pokud není vhodné upravit vaše aplikace tak, aby byly odstraněny afinity zpráv, je k dispozici řada možných řešení problému.

Zadat název určitého místa určení ve volání MQOPEN

Zadejte název vzdálené fronty a název správce front v každém volání produktu MQOPEN a všechny zprávy zařazené do fronty používající tento manipulátor objektu jsou odesílány ke stejnému správci front, což může být lokální správce front.

Zadání názvu vzdálené fronty a názvu správce front pro každé volání MQOPEN má nevýhody:

- Není prováděno žádné vyrovnávání pracovní zátěže. Nevyužívám výhod vyrovnávání pracovní zátěže klastru.
- Je-li cílový správce front vzdálený a existuje více než jeden kanál, zprávy mohou mít různé přenosové cesty a posloupnost zpráv se stále nezachová.
- Pokud má správce front definici pro přenosovou frontu se stejným názvem jako má správce front místa určení, zprávy se raději nepředávají do přenosové fronty klastru a nikoli v přenosové frontě klastru.

Vrátit název správce front v poli správce front pro odpověď

Povolit správci front, který obdrží první zprávu v dávce, vrátit její název ve své odpovědi. To provádí pomocí pole `ReplyToQMgr` deskriptoru zpráv. Správce front na odesílajícím konci pak může extrahovat název správce front odpovědi a zadat jej ve všech následných zprávách.

Použití informací `ReplyToQMgr` z odezvy má nevýhody:

- Žádající správce front musí čekat na odpověď na svou první zprávu
- Chcete-li vyhledat a použít informace o `ReplyToQMgr` před odesláním následných zpráv, musíte napsat další kód.
- Pokud existuje více než jedna přenosová cesta ke správci front, pořadí zpráv nemusí být zachováno

Nastavte volbu `MQOO_BIND_ON_OPEN` u volání `MQOPEN` .

Vynuťte, aby všechny vaše zprávy byly vloženy do stejného cíle pomocí volby `MQOO_BIND_ON_OPEN` na volání `MQOPEN` . 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 určením `MQOO_BIND_ON_OPEN`se vynutí odeslání všech zpráv, které jsou odeslány do této fronty do stejné instance fronty. `MQOO_BIND_ON_OPEN` váže všechny zprávy ke stejnému správci front a také ke stejné přenosové cestě. Je-li například cesta IP a přenosová cesta NetBIOS ke stejnému místu určení, jeden z nich je vybrán při otevření fronty a tento výběr je poctěn pro všechny zprávy zařazené do stejné fronty pomocí získané popisovače objektu.

Zadáním `MQOO_BIND_ON_OPEN` vynuťte, aby všechny zprávy byly směrovány do stejného cíle. Aplikace s afinitními zprávami proto nejsou přerušeny. Není-li místo určení k dispozici, zprávy zůstanou v přenosové frontě, dokud nebude znovu k dispozici.

`MQOO_BIND_ON_OPEN` platí také tehdy, je-li název správce front zadán v deskriptoru objektu při otevření fronty. Jmenovaným správcem front může být více než jedna trasa. Například může existovat více cest k síti nebo jiný správce front může definovat alias. Zadáte-li `MQOO_BIND_ON_OPEN`, je při otevření fronty vybrána přenosová cesta.

Poznámka: Toto je doporučená technika. Nepracuje však v konfiguraci s více přechody, v níž správce front upozorní na alias pro frontu klastru. Nepomáhá ani v situacích, kdy aplikace používají různé fronty ve stejném správci front pro různé skupiny zpráv.

Alternativou k určení `MQOO_BIND_ON_OPEN` ve volání `MQOPEN` je úprava definic front. V definicích front zadejte `DEFBIND(OPEN)` a povolte volbu `DefBind` na volání `MQOPEN` jako standardní nastavení na `MQOO_BIND_AS_Q_DEF`.

Nastavte volbu `MQOO_BIND_ON_GROUP` u volání `MQOPEN` .

Vynuťte, aby všechny zprávy ve skupině byly vloženy do stejného cíle pomocí volby `MQOO_BIND_ON_GROUP` na volání `MQOPEN` . 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 určením `MQOO_BIND_ON_GROUP`se vynutí odeslání všech zpráv ve skupině, které jsou odeslány do této fronty, do stejné instance fronty. `MQOO_BIND_ON_GROUP` váže všechny zprávy ve skupině ke stejnému správci front a také ke stejné přenosové cestě. Pokud například existuje přenosová cesta IP a přenosová cesta NetBIOS do stejného cíle, jeden z nich je vybrán při otevření fronty a tento výběr je poctěn pro všechny zprávy ve skupině zařazené do stejné fronty pomocí získávané popisovače objektu.

Zadáním `MQOO_BIND_ON_GROUP` vynuťte, aby všechny zprávy ve skupině byly směrovány do stejného cíle. Aplikace s afinitními zprávami proto nejsou přerušeny. Není-li místo určení k dispozici, zprávy zůstanou v přenosové frontě, dokud nebude znovu k dispozici.

`MQOO_BIND_ON_GROUP` platí také tehdy, je-li název správce front zadán v deskriptoru objektu při otevření fronty. Jmenovaným správcem front může být více než jedna trasa. Například může existovat více cest

k síti nebo jiný správce front může definovat alias. Zadáte-li MQOO_BIND_ON_GROUP, je při otevření fronty vybrána přenosová cesta.

Aby byl produkt MQOO_BIND_ON_GROUP efektivní, musíte zahrnout volbu vložení MQPMO_LOGICAL_ORDER do MQPUT. Můžete nastavit **GroupId** v MQMD zprávy na MQGI_NONEa v poli MQMD **MsgFlags** zprávy musíte zahrnout následující příznaky zpráv:

- Poslední zpráva ve skupině: MQMF_LAST_MSG_IN_GROUP
- Všechny ostatní zprávy ve skupině: MQMF_MSG_IN_GROUP

Je-li zadán parametr MQOO_BIND_ON_GROUP , ale zprávy nejsou seskupeny, chování je ekvivalentní hodnotě MQOO_BIND_NOT_FIXED.

Poznámka: Toto je doporučená metoda pro ujištění, že zprávy ve skupině jsou odeslány do stejného cíle. Nepracuje však v konfiguraci s více přechody, v níž správce front upozorní na alias pro frontu klastru.

Alternativou k určení MQOO_BIND_ON_GROUP ve volání MQOPEN je úprava definic front. V definicích front zadejte DEFBIND(GROUP) a povolte volbu DefBind na volání MQOPEN jako standardní nastavení na MQOO_BIND_AS_Q_DEF.

Napište přizpůsobený výstupní program pracovní zátěže klastru

Místo úpravy aplikací můžete problém s afinitními zprávami obcházet tím, že napíšete uživatelský program pracovní zátěže klastru. Psaní uživatelského programu pracovní zátěže klastru není snadné a není to doporučené řešení. Program by měl být navržen tak, aby rozpoznal afinitu zkoumáním obsahu zpráv. Po rozpoznání afinity by tento program musel vynutit, aby obslužný program správy pracovní zátěže přesměroval všechny související zprávy do stejného správce front.

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 publikací/odběru ve frontě najdete v následujících dílčích tématech:
  - “Nastavení atributů zpráv publikování/odběru ve frontě” na stránce 381
  - “Spouštění publikování/odběru ve frontě” na stránce 383
  - “Zastavení publikování/odběru ve frontě” na stránce 383
  - “Přidání proudu” na stránce 384
  - “Odstranění proudu” na stránce 385
  - “Přidání bodu odběru” na stránce 385
  - “Kombinování prostorů témat v sítích typu publikování/odběr” na stránce 393

Nastavení atributů zpráv publikování/odběru ve frontě

Chování některých atributů publikování/odběru atributů můžete řídit pomocí atributů správce front. Další atributy, které budete řídit ve stanze *Broker* souboru qm.ini .

Informace o této úloze

Můžete nastavit následující atributy publikování/odběru: podrobnosti viz Parametry správce front .

Tabulka 28. Konfigurační parametry publikování a odběru

Popis	**Název parametru MQSC**
Počet opakování zprávy příkazu	**PSRTYCNT**

Tabulka 28. Konfigurační parametry publikování a odběru (pokračování)	
Popis	**Název parametru MQSC**
Zahodit nedoručitelnou vstupní zprávu příkazu	**PSNPMSG**
Chování po nedoručitelné zprávě s odpovědí příkazu	**PSNPRES**
Zprávy příkazů zpracování v synchronizačním bodě	**PSSYNCPT**

Sekce Zprostředkovatel se používá ke správě následujících nastavení konfigurace:

- `PersistentPublishRetry=yes | force`

  Pokud uvedete `Yes`, pak pokud se nezdaří publikování trvalé zprávy prostřednictvím rozhraní publikování/odběru ve frontě a nebyla požadována žádná záporná odpověď, operace publikování se zopakují.

  Pokud jste si vyžádali negativní odezvu, odešle se negativní odezva a nedojde k dalšímu opakování.

  Zadáte-li volbu `Vynutit`, dojde-li k selhání publikování trvalé zprávy prostřednictvím rozhraní publikování/odběru ve frontě, bude operace publikování zopakována, dokud nebude úspěšně zpracována. Neodešle se žádná negativní odezva.

- `NonPersistentPublishRetry= ano | force`

  Pokud uvedete `Yes`, pak pokud selže publikování dočasné zprávy prostřednictvím rozhraní publikování/odběru ve frontě, a nebyla požadována žádná negativní odpověď, operace publikování se zopakuje.

  Pokud jste si vyžádali negativní odezvu, odešle se negativní odezva a nedojde k dalšímu opakování.

  Pokud jste určili volbu `Vynutit`, dojde k selhání publikování netrvalé zprávy prostřednictvím rozhraní publikování/odběru ve frontě, operace publikování bude zopakována, dokud nebude úspěšně zpracována. Neodešle se žádná negativní odezva.

  Poznámka: Chcete-li povolit tuto funkci pro netrvalé zprávy a také nastavit hodnotu `NonPersistentPublishRetry` , musíte také zajistit, aby byl atribut správce front **PSSYNCPT** nastaven na hodnotu `Ano`.

  Provedení této akce může mít také vliv na výkon dočasných publikování, protože **MQGET** ze fronty STREAM se nyní vyskytuje pod synchronizačním bodem.

- `PublishBatchVelikost =`*`číslo`*

  Zprostředkovatel normálně zpracovává zprávy publikování v rámci synchronizačního bodu. Může být neefektivní potvrdit každou publikaci individuálně, a za určitých okolností může zprostředkovatel zpracovávat více publikovaných zpráv v jediné transakci. Tento parametr určuje maximální počet zpráv publikování, které lze zpracovat v jedné pracovní jednotce.

  Výchozí hodnota parametru `PublishBatchSize` je 5.

- `PublishBatchInterval =`*`číslo`*

  Zprostředkovatel normálně zpracovává zprávy publikování v rámci synchronizačního bodu. Může být neefektivní potvrdit každou publikaci individuálně, a za určitých okolností může zprostředkovatel zpracovávat více publikovaných zpráv v jediné transakci. Tento parametr uvádí maximální dobu (v milisekundách) mezi první zprávou v dávce a jakoukoli následnou publikací zahrnutou do stejné dávky.

  Interval dávek 0 označuje, že lze zpracovat až `PublishBatchVelikost` zpráv za předpokladu, že tyto zprávy jsou okamžitě k dispozici.

  Výchozí hodnota parametru `PublishBatchInterval` je nula.

Postup

Pomocí Průzkumníka IBM MQ , programovatelných příkazů nebo pomocí příkazu **runmqsc** můžete změnit atributy správce front, které řídí chování publish/odběru.

Příklad

ALTER QMGR PSNPRES (SAFE)

Spouštění publikování/odběru ve frontě

Publikování/odběr ve frontě můžete spustit 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 se spouštěl buď rozhraní publikování/odběru ve frontě (známé také jako zprostředkovatel), nebo stroj publikování/odběru (také známý jako publish/subscribe verze 7) nebo obojí. Chcete-li zahájit publikování/odběr ve frontě, je třeba nastavit parametr PSMODE na hodnotu ENABLED. Výchozí hodnota je ENABLED.

Postup

Použijte příkaz IBM MQ Explorer nebo **runmqsc** , abyste povolili rozhraní publikování/odběru ve frontě, pokud toto rozhraní ještě není povoleno.

Příklad

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

Jak pokračovat dále

Procesy produktu IBM MQ zařazují do fronty příkazy publikování/odběru ve frontě a volání rozhraní MQI (Message Queue Queue Interface) publikování/odběru.

Zastavení publikování/odběru ve frontě

Publikování/odběr ve frontě můžete zastavit 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 se zastavil buď rozhraní publikování/odběru ve frontě (známé také jako zprostředkovatel), nebo stroj publikování/odběru (také známý jako publish/subscribe verze 7) nebo obojí. Chcete-li ukončit publikování/odběr ve frontě, je třeba nastavit parametr PSMODE na hodnotu COMPAT. Chcete-li zcela zastavit stroj publikování/odběru, nastavte PSMODE na DISABLED.

Postup

Chcete-li zakázat rozhraní publikování/odběru ve frontě, použijte příkaz IBM MQ Explorer nebo příkaz **runmqsc** .

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 WebSphere MQ 6 .

Než začnete

Seznamte se s tím, jak fungují proudy publikování/odběru. Viz Proudy a témata.

Informace o této úloze

K provedení těchto kroků použijte příkaz PCF, **runmqsc**nebo 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 IBM WebSphere MQ 6 .
2. Definujte lokální téma se stejným názvem jako proud IBM WebSphere MQ 6 .
3. Přidejte název fronty do seznamu názvů SYSTEM.QPUBSUB.QUEUE.NAMELIST .
4. Opakujte pro všechny správce front v adresáři IBM WebSphere MQ 7.1 nebo vyšším, kteří jsou v hierarchii publikování/odběru.

přidání 'Sport'

V příkladu sdílení proudu 'Sport', IBM WebSphere MQ 6 a IBM WebSphere MQ 7.1 správci front pracují ve stejné hierarchii publikování/odběru. Správci front IBM WebSphere MQ 6 sdílejí proud s názvem 'Sport'. Příklad ukazuje, jak vytvořit frontu a téma na IBM WebSphere MQ 7.1 správcích front s názvem 'Sport's řetězcem tématu 'Sport' , který je sdílen s IBM WebSphere MQ 6 proudem 'Sport'.

IBM WebSphere MQ 7.1 Publikační aplikace, publikování do tématu 'Sport', s řetězcem tématu 'Soccer/Results', vytvoří výsledný řetězec tématu 'Sport/Soccer/Results'. Ve správcích front systému IBM WebSphere MQ 7.1 obdrží publikování odběratelé tématu 'Sport's řetězcem tématu 'Soccer/Results' .

Ve správcích front systému IBM WebSphere MQ 6 obdrží publikování odběratelé pro proud 'Sport's řetězcem tématu 'Soccer/Results' .

```
runmqsc QM1
5724-H72 (C) Copyright IBM Corp. 1994, 2024.  ALL RIGHTS RESERVED.
Starting MQSC for queue manager QM1.
define qlocal('Sport')
     1 : define qlocal('Sport')
AMQ8006: 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.

Pokud je zprostředkovatel verze 6, spravujte jej jako zprostředkovatele IBM WebSphere MQ 6 . To znamená, že máte možnost vytvořit frontu proudu ručně nebo nechat zprostředkovatele vytvořit frontu proudu dynamicky v případě potřeby. Fronta je založena na definici modelové fronty `SYSTEM.BROKER.MODEL.STREAM`.

Je-li zprostředkovatel verze 71, musíte nakonfigurovat každého správce front IBM WebSphere MQ 7.1 v hierarchii ručně.

Odstranění proudu

Proud můžete odstranit ze správce front produktu IBM WebSphere MQ 7.1nebo novější.

Než začnete

Před odstraněním proudu se musíte ujistit, že neexistují žádné zbývající odběry proudu a uvede se do klidového stavu všechny aplikace, které tento proud používají. Pokud publikace pokračují v toku do odstraněného proudu, trvá mnoho administrativních sil k obnově systému do vyčištěného pracovního stavu.

Postup

1. Najít všechny připojené zprostředkovatele, kteří jsou hostiteli tohoto proudu.
2. Zrušit všechny odběry proudu na všech zprostředkovatelů.
3. Odeberte frontu ze seznamu názvů (se stejným názvem jako proud), `SYSTEM.QPUBSUB.QUEUE.NAMELIST`.
4. Odstraňte nebo vymažte všechny zprávy z fronty se stejným názvem jako má proud.
5. Odstraňte frontu se stejným názvem, jako má proud.
6. Odstranit přidružený objekt tématu.

Jak pokračovat dále

Zopakujte kroky 3 až 5 ve všech ostatních propojeném produktu IBM WebSphere MQ 7.1nebo novějším, kteří jsou hostiteli proudu.

Přidání bodu odběru

Jak rozšířit existující aplikaci publikování/odběru ve frontě, kterou jste migrovali ze starší verze produktu IBM Integration Bus s novým bodem odběru.

Než začnete

1. Ověřte, že bod odběru není v produktu `SYSTEM.QPUBSUB.SUBPOINT.NAMELIST`již definován.
2. Zkontrolujte, zda existuje objekt tématu nebo řetězec tématu se stejným názvem jako bod odběru.

Informace o této úloze

Aplikace IBM WebSphere MQ 7.1nebo novější aplikace nepoužívají body odběru, ale mohou spolupracovat s existujícími aplikacemi, které používají mechanizmus migrace bodu odběru.

Důležité: Mechanismus migrace bodu odběru byl odebrán z produktu IBM MQ 8.0. Potřebujete-li migrovat existující aplikace, musíte před migrací na nejnovější verzi provést procedury popsané v dokumentaci pro vaši verzi produktu.

Body odběru nepracují s programy publikování/odběru ve frontě, které používají záhlaví produktu `MQRFH1` , která byla migrována z produktu IBM WebSphere MQ 6nebo starší.

Není třeba přidávat body odběru pro použití integrovaných aplikací publikování/odběru, které jsou napsány pro produkt IBM WebSphere MQ 7.1nebo novější.

Postup

1. Přidejte název bodu odběru do produktu SYSTEM.QPUBSUB.SUBPOINT.NAMELIST.
   - V systému z/OSje hodnota **NLTYPE** nastavena na hodnotu NONE(výchozí hodnota).
   - Opakujte tento krok u všech správců front, kteří jsou připojeni ve stejné topologii publikování/odběru.
2. Přidejte objekt tématu, pokud možno jej pojmenujte s názvem bodu odběru, s řetězcem tématu, který odpovídá názvu bodu odběru.
   - Je-li bod odběru umístěn v klastru, přidejte objekt tématu jako téma klastru na hostitele tématu klastru.
   - Pokud objekt tématu existuje se stejným řetězcem tématu jako název bodu odběru, použijte existující objekt tématu. Musíte pochopit důsledky bodu odběru opětovným použitím existujícího tématu. Je-li existující téma součástí existující aplikace, je nutné vyřešit kolizi mezi dvěma identicky pojmenovanými tématy.
   - Existuje-li objekt tématu se stejným názvem jako bod odběru, ale jiný řetězec tématu, vytvořte téma s jiným názvem.
3. Nastavte atribut **Topic** WILDCARD na hodnotu BLOCK.

   Zablokování odběrů pro zástupné znaky # nebo * izolují zástupný znak na body odběru, viz Zástupné znaky a body odběru.
4. Nastavte všechny atributy, které vyžadujete v objektu tématu.

Příklad

Tento příklad ukazuje příkazový soubor **runmqsc** , který přidává dva body odběru, USD a GBP.

```
DEFINE TOPIC(USD) TOPICSTR(USD)
DEFINE TOPIC(GBP) TOPICSTR(GBP) WILDCARD(BLOCK)
ALTER NL(SYSTEM.QPUBSUB.SUBPOINT.NAMELIST) NAMES(SYSTEM.BROKER.DEFAULT.SUBPOINT, USD, GBP)
```

Poznámka:

1. Přidejte výchozí bod odběru do seznamu bodů odběru přidaných pomocí příkazu **ALTER** . Příkaz **ALTER** odstraní existující názvy v seznamu názvů.
2. Před změnou seznamu názvů definujte témata. Správce front kontroluje seznam názvů pouze v případě, že je spuštěn správce front a kdy je seznam názvů změněn.

Konfigurace sítí distribuovaných publikování/odběru

Správci front, kteří jsou připojeni k distribuované topologii publikování/odběru, sdílejí společný federovaný prostor tématu. Odběry vytvořené v jednom správci front mohou přijímat zprávy publikované aplikací připojenou k jinému správci front v rámci topologie.

Rozsah prostorů témat vytvořených připojováním správců front v klastrech nebo hierarchiích můžete řídit rozsah vytvořených prostorů témat. V klastru publikování/odběru musí být objekt tématu "klastrovaný" pro každou větev prostoru tématu, který má být rozdělen do klastru. V hierarchii musí být každý správce front nakonfigurován pro identifikaci svého 'nadřízeného' v hierarchii.

Tok publikování a odběrů v rámci topologie můžete dále řídit výběrem toho, zda jsou jednotlivé publikace a odběry buď lokální, nebo globální. Lokální publikování a odběry nejsou šířeny mimo správce front, k němuž je vydavatel nebo odběratel připojen.

Související pojmy

Distribuované sítě typu publikování/odběr

Obor publikování

Obor odběru
Prostory tématu
Související úlohy
Definování témat klastru

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Než začnete

Některé konfigurace klastru nemohou pojmout režijní náklady přímého přesměrovaného publikování/odběru. Před použitím této konfigurace prozkoumejte aspekty a volby popsané v tématu Navrhování klastrů publikování a odběru.

Aby se změny v klastru rozšířily do celého klastru, musí být vždy k dispozici alespoň jedno úplné úložiště. Před spuštěním této úlohy zkontrolujte, zda jsou vaše úložiště k dispozici.

Viz také Směrování pro klastry publikování/odběru: Notes on chování.

Scénář:

- Klastr INVENTORY byl nastaven tak, jak je popsáno v tématu “Přidání správce front do klastru” na stránce 288. Obsahuje tři správce front; produkty LONDON a NEWYORK obsahují úplná úložiště, produkt PARIS uchovává dílčí úložiště.

Informace o této úloze

Definujete-li téma ve správci front v klastru, je třeba určit, zda se jedná o téma klastru, a (je-li tomu tak) směrování v rámci klastru pro publikování a odběry pro toto téma. Chcete-li provést vytvoření tématu klastru, nakonfigurujte vlastnost **CLUSTER** na objektu TOPIC s názvem klastru. Definováním tématu klastru na správci front v klastru zpřístupníte téma celému klastru. Chcete-li zvolit směrování zpráv, které má být použito v klastru, nastavíte vlastnost **CLROUTE** na 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 téma Přímé 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 téma Klastry publikování/odběru se směrováním hostitele 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 má být hostitelem vašeho tématu.

   Kterýkoli správce front klastru může hostovat téma. Vyberte si jednoho ze tří správců front (LONDON, NEWYORK nebo PARIS) a konfigurujte vlastnosti objektu TOPIC . Plánujete-li používat přímé směrování, nebude již provozní rozdíl mezi vámi a správcem front. Plánujete-li používat směrování hostitelů témat, bude mít vybraný správce front další povinnosti pro směrování publikací. Proto u 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 vytvořit téma klastru, zahrňte název klastru při definování tématu a nastavte směrování, které chcete používat pro publikování a odběry pro toto téma. Chcete-li například vytvořit téma klastru s přímým směrováním ve správci front produktu LONDON , vytvořte následující téma:

   ```
   DEFINE TOPIC(INVENTORY) TOPICSTR('/INVENTORY') CLUSTER(INVENTORY) CLROUTE(DIRECT)
   ```

   Definováním tématu klastru na správci front v klastru zpřístupníte téma celému klastru.

   Další informace o použití příkazu **CLROUTE**naleznete v tématu DEFINE TOPIC (CLROUTE) a Routing pro klastry publikování/odběru: Notes on chování.

Výsledky

Klastr je připraven přijímat publikování a odběry pro dané téma.

Jak pokračovat dále

Pokud jste nakonfigurovali klastr publikování/odběru se směrováním hostitele tématu, pravděpodobně budete chtít pro toto téma přidat další hostitele tématu. Viz “Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu” na stránce 390.

Pokud máte několik samostatných klastrů publikování/odběru, například protože je vaše organizace geograficky rozptýlená, možná budete chtít rozšířit některá témata klastru do všech klastrů. To můžete provést tak, že propojíte klastry v hierarchii. Viz “Sloučení prostorů témat u více klastrů” na stránce 396. Můžete také řídit tok publikací z jednoho klastru do jiného. Viz “Kombinování a izolování prostorů témat ve více klastrech” na stránce 398.

Související pojmy

Kombinování oborů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracuje obor publikování a odběru prací nezávisle na určení toku publikování mezi správci front.

Kombinování prostorů témat v sítích typu publikování/odběr
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

Přesun definice tématu klastru do jiného správce front
Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu
V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou 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 a odběru
Odstraňování problémů distribuovaného publikování/odběru
Blokující publish/odběr v klastru

Přesun definice tématu klastru do jiného správce front

Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Informace o této úloze

V klastru můžete mít více definic jednoho objektu tématu klastru. Jedná se o normální stav pro klastr směrování hostitele témat a neobvyklý stav pro přímo směrovaný klastr. Další informace naleznete v tématu Několik definic tématu klastru se stejným názvem.

Chcete-li přesunout definici tématu klastru do jiného správce front v klastru, aniž byste přerušili tok publikací, postupujte takto. Procedura přesune definici ze správce front QM1 do správce front QM2.

Postup

1. Vytvořte duplikát definice tématu klastru v systému QM2.

   Chcete-li směrovat přímé směrování, nastavte všechny atributy tak, aby odpovídaly definici QM1.

   V případě směrování hostitele témat nejprve definujte nového hostitele tématu jako PUB(DISABLED). To umožňuje programu QM2 získat informace o odběrech v klastru, ale ne při spouštění směrování publikací.
2. Počkejte, až budou informace šířeny prostřednictvím klastru.

   Počkejte, až bude nová definice tématu klastru šířena správci front úplného úložiště do všech správců front v klastru. Použijte příkaz **DISPLAY CLUSTER** k zobrazení témat klastru na každém členu klastru a zkontrolujte definici, která pochází z QM2.

   Chcete-li se dozvědět o všech odběrech, počkejte na směrování hostitele témat na nového hostitele tématu QM2 . Porovnejte proxy odběry známé pro QM2 a ty, které jsou známé uživateli QM1. Jednou z možností, jak zobrazit proxy odběry ve správci front, je zadání následujícího příkazu **runmqsc** :

   ```
   DISPLAY SUB(*) SUBTYPE(PROXY)
   ```
3. Pro směrování hostitele témat změňte název hostitele tématu na QM2 jako PUB(ENABLED)a potom předefinujte hostitele témat na QM1 jako PUB(DISABLED).

   Nyní, když se nový uzel tématu na systému QM2 dozvěděl o všech odběrech na jiných správcích front, může hostitel tématu zahájit směrování publikací.

   Pomocí nastavení PUB(DISABLED) pro uvedení provozu zpráv do klidového stavu pomocí QM1zajistíte, že žádné publikace nebudou ve vlaku přes QM1 , když odstraníte definici tématu klastru.
4. Odstraňte definici tématu klastru z QM1.

   Definici můžete odstranit pouze z QM1 , je-li správce front k dispozici. Jinak musíte pracovat s oběma definicemi, dokud nebude QM1 restartováno nebo vynuceno odebrání.

   Pokud QM1 zůstane nedostupný po dlouhou dobu a během této doby je třeba upravit definici klastrovaného tématu v systému QM2, definice QM2 je novější než definice QM1 , a proto obvykle převládne.

Pokud v tomto období existují rozdíly mezi definicemi v systému QM1 a QM2, dojde k zápisu chyb do protokolů chyb obou správců front, které vás upozorní na konfliktní definici tématu klastru.

Pokud se QM1 nikdy nevrátí do klastru, například kvůli neočekávanému vyřazení z provozu po selhání hardwaru, jako poslední možnost můžete použít příkaz RESET CLUSTER k vynucenému vysunutí správce front. Příkaz **RESET CLUSTER** automaticky odstraní všechny objekty témat, které jsou hostovány v cílovém správci front.

Související pojmy

Kombinování oborů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracuje obor publikování a odběru prací nezávisle na určení toku publikování mezi správci front.

Kombinování prostorů témat v sítích typu publikování/odběr
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu
V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou 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 směrováním hostitele tématu

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou směrovat přes nového hostitele tématu.

Než začnete

Definování stejného objektu tématu klastru v několika správcích front je funkčně užitečné pouze pro klastr se směrováním hostitele tématu. Definování více shodujících se témat v klastru s přímým směrováním nezmění své chování. Tato úloha se týká pouze klastrů se směrováním hostitele tématu.

Tato úloha předpokládá, že jste si přečetli článek Více definic tématu klastru se stejným názvem, a to zejména v následujících sekcích:

- Více definic tématu klastru v klastru se směrováním hostitelů témat
- Speciální zacházení pro parametr PUB

Informace o této úloze

Je-li správce front přesměrován na hostitele témat, musí se nejprve dozvědět o existenci všech souvisejících témat, která jsou přihlášena k odběru v klastru. Pokud jsou publikace publikovány do těchto

témat v době, kdy je přidán další hostitel tématu, a publikování je přesměrováno na nového hostitele před tím, než se tento hostitel dozvěděl o existenci odběrů u jiných správců front v klastru, nebude tento nový hostitel přesměrován na tyto odběry. To způsobí, že odběry chybí publikování.

Publikace nejsou směrovány přes správce front hostitele tématu, kteří výslovně nastavili parametr objektu tématu klastru **PUB** na hodnotu DISABLED, takže toto nastavení můžete použít k zajištění toho, aby žádné odběry neuniklo během procesu přidávání dalšího hostitele témat.

Poznámka: Zatímco správce front je hostitelem tématu klastru, které bylo definováno jako PUB(DISABLED), vydavatelé připojené k tomuto správci front nemohou publikovat zprávy a odpovídající odběry v tomto správci front nepřijímají publikování publikovaná v jiných správcích front v klastru. Z tohoto důvodu je třeba pečlivě zvážit definování témat směrována hostitelem tématu u správců front, kde existují odběry a publikování aplikací.

Postup

1. Nakonfigurujte nového hostitele tématu a na počátku definujte nového hostitele tématu jako PUB(DISABLED).

   To umožňuje novému hostiteli témat informace o odběrech v klastru, ale ne ke spuštění směrování publikací.

   Informace o konfiguraci hostitele témat viz “Konfigurace klastru publikování/odběru” na stránce 387.
2. Určete, kdy se nový hostitel tématu dozvěděl o všech odběrech.

   Chcete-li tak učinit, porovnejte proxy odběry známé pro nového hostitele témat a ty, které jsou známy existujícím hostitelům témat. Jednou z možností, jak zobrazit proxy odběry, je vydat následující příkaz **runmqsc** : DISPLAY SUB(*) SUBTYPE(PROXY)
3. Předefinujte nového hostitele tématu jako PUB(ENABLED).

   Poté, co se nový uzel tématu dozvěděl o všech odběrech na jiných správcích front, může téma zahájit směrování publikací.

Související pojmy

Kombinování oborů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracuje obor publikování a odběru prací nezávisle na určení toku publikování mezi správci front.

Kombinování prostorů témat v sítích typu publikování/odběr
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesun definice tématu klastru do jiného správce front
Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Připojení správce front k hierarchii publikování/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.

Kombinování oborů publikování a odběrů

Počínaje produktem IBM WebSphere MQ 7.0 pracuje obor publikování a odběru prací nezávisle na určení toku publikování mezi správci front.

Publikování mohou přejít do všech správců front, kteří jsou připojeni k topologii publikování/odběru nebo pouze lokálnímu správci front. Podobně pro proxy odběry. Informace o tom, které publikace odpovídají odběru, se řídí kombinací těchto dvou toků.

Publikování a odběry mohou mít rozsah hodnot QMGR nebo ALL. Pokud je vydavatel a odběratel připojen ke stejnému správci front, neovlivňují nastavení rozsahu publikování, která odběratel obdrží od tohoto vydavatele.

Pokud je vydavatel a odběratel připojeni k různým správcům front, obě nastavení musí být VŠE , aby bylo možné přijímat vzdálená publikování.

Předpokládejme, že vydavatelé jsou připojeni k různým správcům front. Pokud chcete, aby odběratel přijímal publikování od libovolného vydavatele, nastavte rozsah odběru na hodnotu VŠE. Poté můžete rozhodnout pro každého vydavatele, zda má být omezen rozsah jeho publikací na odběratele lokální pro vydavatele.

Předpokládejme, že odběratelé jsou připojeni k různým správcům front. Pokud chcete, aby byly publikace od vydavatele odeslány všem odběratelům, nastavte rozsah publikování na hodnotu VŠE. Chcete-li odběratele přijímat publikování pouze od vydavatele připojeného ke stejnému správci front, nastavte rozsah odběru na QMGR.

Příklad: služba fotbalových výsledků

Předpokládejme, že jste členský tým ve fotbalové lize. Každý tým má k dispozici správce front připojený ke všem ostatním týmům v klastru publikování/odběru.

Týmy publikují výsledky všech her hraných na jejich domovské zemi pomocí tohoto tématu, `Football/result/`*`Home team name/Away team name`*. Řetězce psané kurzívou jsou variabilní názvy témat a publikování je výsledkem shody.

Každý klub také znovu publikuje výsledky pouze pro klub s použitím řetězce tématu `Football/myteam/`*`Home team name/Away team name`*.

Obě témata jsou publikována v celém klastru.

Následující odběry byly vytvořeny v lize tak, že fanoušci libovolného týmu se mohou přihlásit k odběru výsledků ve třech zajímavých ohledech.

Všimněte si, že můžete nastavit témata klastru pomocí produktu SUBSCOPE(QMGR). Definice tématu se šíří do každého člena klastru, ale rozsah odběru je pouze lokální správce front. Odběratelé v každém správci front proto obdrží od stejného odběru různé publikace.

Přijmout všechny výsledky

```
DEFINE TOPIC(A) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(ALL)
```

Přijmout všechny domovské výsledky

```
DEFINE TOPIC(B) TOPICSTR('Football/result/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR , jsou porovnávány pouze výsledky publikované v domovském umístění.

Přijmout všechny výsledky mých týmů

```
DEFINE TOPIC(C) TOPICSTR('Football/myteam/') CLUSTER SUBSCOPE(QMGR)
```

Vzhledem k tomu, že odběr má rozsah QMGR , budou porovnávány pouze lokální výsledky týmu, které se znovu publikují lokálně.

Související pojmy

Kombinování prostorů témat v sítích typu publikování/odběr
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Distribuované sítě typu publikování/odběr

Obor publikování

Obor odběru

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesun definice tématu klastru do jiného správce front
Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu
V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou 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.

Kombinování prostorů témat v sítích typu publikování/odběr

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Můžete vytvořit různé prostory tématu pro publikování/odběr pomocí stavebních bloků atributů **CLUSTER**, **PUBSCOPE** a **SUBSCOPE** , klastrů typu publikování/odběr a publikování/odběru hierarchií.

Při spuštění z příkladu změny měřítka z jednoho správce front do klastru publikování/odběru, následující scénáře ilustrují různé topologie publikování/odběru.

Související pojmy

Kombinování oborů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracuje obor publikování a odběru prací nezávisle na určení toku publikování mezi správci front.

Distribuované sítě typu publikování/odběr

Prostory tématu

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesun definice tématu klastru do jiného správce front
Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu
V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou 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 jediného prostoru tématu v klastru publikování/odběru

Rozšiřte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

Než začnete

Naimplementovali jste systém typu publikování-odběr u jednoho správce front verze 7.

Vždy vytvářejte prostory tématu s vlastními uživateli root, spíše než spoléháte na dědění atributů produktu `SYSTEM.BASE.TOPIC`. Pokud škálujete systém publikování/odběru do klastru, můžete definovat kořenové témata jako témata klastru, na hostiteli témat klastru a poté všechny vaše témata sdílet v rámci celého klastru.

Informace o této úloze

Nyní chcete rozšířit systém tak, aby podporoval více vydavatelů a odběratelů a aby měl každé téma viditelné v rámci celého klastru.

Postup

1. Vytvořte klastr, který má být použit se systémem publikování/odběru.

   Máte-li existující tradiční klastr, z důvodu výkonu je lepší nastavit nový klastr pro nový systém odběru publikování. Pro úložiště klastru u obou klastrů můžete použít stejné servery.
2. Vyberte jednoho správce front, pravděpodobně jednoho z úložišť, který bude hostitelem tématu klastru.
3. Ujistěte se, že každé téma, které má být viditelné v rámci klastru publikování/odběru, se interpretuje jako objekt tématu administrace.
   Nastavte atribut **CLUSTER** pro pojmenování klastru publikování/odběru.

Jak pokračovat dále

Připojte vydavatele a aplikace odběratele do všech správců front v klastru.

Vytvořte objekty administrativního tématu, které mají atribut **CLUSTER** . Témata se také šíří do celého klastru. Programy vydavatele a odběratele používají administrativní témata, aby jejich chování nebylo změněno tím, že je připojeno k různým správcům front v klastru.

Pokud potřebujete produkt `SYSTEM.BASE.TOPIC` v každém správci front vystupovat jako téma klastru, je třeba jej upravit ve všech správci front.

Související pojmy

Distribuované sítě typu publikování/odběr

Prostory tématu

Související úlohy

Přidání správce front produktu IBM WebSphere MQ 7 nebo novější do existujících prostorů témat IBM WebSphere MQ 6
Rozšiřte existující systém publikování/odběru produktu IBM WebSphere MQ 6 tak, aby spolupracovat s produktem IBM WebSphere MQ 7 nebo novějším správcem front a sdílel stejné prostory témat.

Sloučení prostorů témat u více klastrů
Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Kombinování a izolování prostorů témat ve více klastrech
Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

Publikování a přihlášení k odběru prostorů témat ve více klastrech
Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Definování témat klastru

Přidání správce front produktu IBM WebSphere MQ 7 nebo novější do existujících prostorů témat IBM WebSphere MQ 6

Rozšiřte existující systém publikování/odběru produktu IBM WebSphere MQ 6 tak, aby spolupracovat s produktem IBM WebSphere MQ 7 nebo novějším správcem front a sdílel stejné prostory témat.

Než začnete

You have an existing IBM WebSphere MQ 6 publish/subscribe system.

Nainstalovali jste produkt IBM WebSphere MQ 7 nebo novější na nový server a nakonfigurovali jste správce front.

Informace o této úloze

You want to extend your existing IBM WebSphere MQ 6 publish/subscribe system to work with IBM WebSphere MQ 7 or later queue managers.

Rozhodli jste se stabilizovat vývoj systému publikování/odběru IBM WebSphere MQ 6 , který používá rozhraní publikování/odběru ve frontě. Zamýšlíte přidat rozšíření do systému pomocí produktu IBM WebSphere MQ 7 nebo pozdějšího MQI. Nyní nemáte žádné plány na přepsání aplikací publikování/odběru ve frontě.

Máte v úmyslu upgradovat správce front produktu IBM WebSphere MQ 6 na produkt IBM WebSphere MQ 7 nebo později v budoucnu. Prozatím nadále spouštíte existující aplikace publikování/odběru ve frontě na správcích front produktu IBM WebSphere MQ 7 nebo novější.

Postup

1. Vytvořte jednu sadu přijímacích kanálů odesílatele pro připojení správce front verze 7 nebo novější k jednomu ze správců front produktu IBM WebSphere MQ 6 v obou směrech.
2. Vytvořte dvě přenosové fronty s názvy cílových správců front. Alias správce front použijte, pokud z nějakého důvodu nelze použít název cílového správce front jako název přenosové fronty.
3. Konfigurujte přenosové fronty tak, aby spustily odesílací kanály.
4. Pokud systém publikování/odběru IBM WebSphere MQ 6 používá proudy, přidejte proudy do správce front verze 7 nebo vyšší, jak je popsáno v tématu “Přidání proudu” na stránce 384.
5. Zkontrolujte, zda je správce front verze 7 nebo novější **PSMODE** nastaven na hodnotu ENABLE.
6. Změňte její atribut **PARENT** tak, aby odkazoval na jednoho ze správců front produktu IBM WebSphere MQ 6 .
7. Zkontrolujte, zda je stav relace nadřízený-podřízený mezi správci front aktivní v obou směrech.

Jak pokračovat dále

Po dokončení úlohy produkt IBM WebSphere MQ 6 i správce front produktu IBM WebSphere MQ 7 nebo novější sdílejí stejné prostory témat. Můžete například provést všechny následující úlohy.

- Výměna publikací a odběrů mezi produkty IBM WebSphere MQ 6 a IBM WebSphere MQ 7 nebo pozdější správci front.
- Spusťte existující programy typu IBM WebSphere MQ 6 publish/subscribe ve správci front produktu IBM WebSphere MQ 7 nebo pozdější.
- Zobrazte a upravte prostor tématu buď na serveru IBM WebSphere MQ 6 , nebo na správci front produktu IBM WebSphere MQ 7 nebo na vyšší úrovni.
- Zapište IBM WebSphere MQ 7 nebo pozdější publikování/odběr aplikací a spusťte je na správci front produktu IBM WebSphere MQ 7 nebo novější.
- Vytvářejte nové publikace a odběry s aplikacemi produktu IBM WebSphere MQ 7 nebo pozdější a vyměňujete je s aplikacemi produktu IBM WebSphere MQ 6 .

Související pojmy

Distribuované sítě typu publikování/odběr

Prostory tématu

Související úlohy

Vytvoření jediného prostoru tématu v klastru publikování/odběru
Rozšiřte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

Sloučení prostorů témat u více klastrů
Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Kombinování a izolování prostorů témat ve více klastrech
Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

Publikování a přihlášení k odběru prostorů témat ve více klastrech
Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Definování témat klastru

Sloučení prostorů témat u více klastrů

Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Než začnete

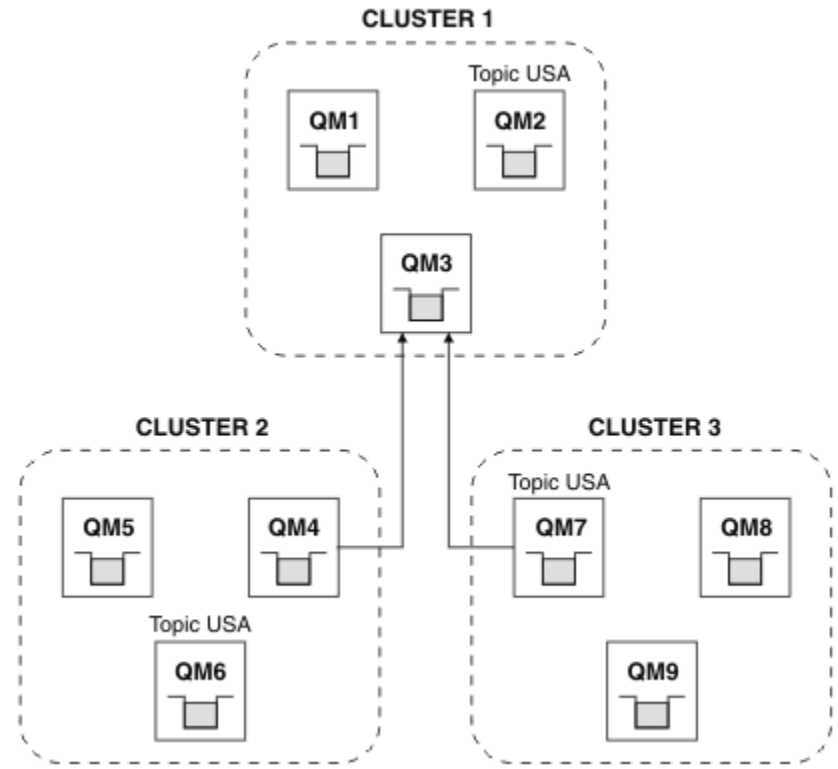
Tato úloha předpokládá, že máte existující přímo směrované klastry publikování/odběru, a chcete šířit některá témata klastru do všech klastrů.

Poznámka: To nelze provést pro klastry publikování/odběru se směrováním hostitelů/odběru.

Informace o této úloze

Chcete-li šířit publikace z jednoho klastru do jiného, musíte se připojit ke klastrům společně v hierarchii; viz Obrázek 67 na stránce 397. Hierarchická připojení šíří odběry a publikování mezi propojenými správci front a klastry šíří témata klastru v rámci jednotlivých klastrů, ale nikoli mezi klastry.

Kombinace těchto dvou mechanismů šíří témata klastru mezi všemi klastry. Je třeba, abyste v každém klastru zopakovali definice tématu klastru.



Obrázek 67. Připojování klastrů pomocí hierarchií

Následující kroky spojují klastry do hierarchie.

Postup

1. Vytvořte dvě sady přijímacích kanálů odesílatele k připojení produktů QM3 a QM4a QM3 a QM7v obou směrech. Chcete-li připojit hierarchii, musíte použít tradiční odesílací kanály odesílatele a přenosové fronty, spíše než klastr.
2. Vytvořte tři přenosové fronty s názvy cílových správců front. Alias správce front použijte, pokud z nějakého důvodu nelze použít název cílového správce front jako název přenosové fronty.
3. Konfigurujte přenosové fronty tak, aby spustily odesílací kanály.
4. Zkontrolujte, zda je **PSMODE** z QM3, QM4 a QM7 nastaveno na ENABLE.
5. Pozměňte atribut **PARENT** z QM4 a QM7 na QM3.
6. Zkontrolujte, zda je stav relace 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') na každém ze tří správců front hostitele tématu klastru v klastrech 1, 2 a 3. Hostitele tématu klastru nemusí být hierarchicky připojeným správcem front.

Jak pokračovat dále

Nyní můžete publikovat nebo přihlásit se k odběru tématu klastru USA v produktu Obrázek 67 na stránce 397. Publikování odběrů publikování pro vydavatele a odběratele ve všech třech klastrech.

Předpokládejme, že jste nevytvořili USA jako téma klastru v ostatních klastrech. Je-li USA definováno pouze v systému QM7, jsou publikace a odběry USA vyměňovány mezi QM7, QM8, QM9a QM3. Vydavatelé a odběratelé spuštění v systému QM7, QM8, QM9 dědí atributy administrativního tématu USA. Vydavatelé a odběratelé na QM3 dědí atributy z SYSTEM.BASE.TOPIC na QM3.

Další informace najdete v tématu “Kombinování a izolování prostorů témat ve více klastrech” na stránce 398.

Související pojmy

Distribuované sítě typu publikování/odběr

Prostory tématu

Související úlohy

Vytvoření jediného prostoru tématu v klastru publikování/odběru
Rozšiřte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

Přidání správce front produktu IBM WebSphere MQ 7 nebo novější do existujících prostorů témat IBM WebSphere MQ 6
Rozšiřte existující systém publikování/odběru produktu IBM WebSphere MQ 6 tak, aby spolupracovat s produktem IBM WebSphere MQ 7 nebo novějším správcem front a sdílel stejné prostory témat.

Kombinování a izolování prostorů témat ve více klastrech
Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

Publikování a přihlášení k odběru prostorů témat ve více klastrech
Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Definování témat klastru

Kombinování a izolování prostorů témat ve více klastrech

Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

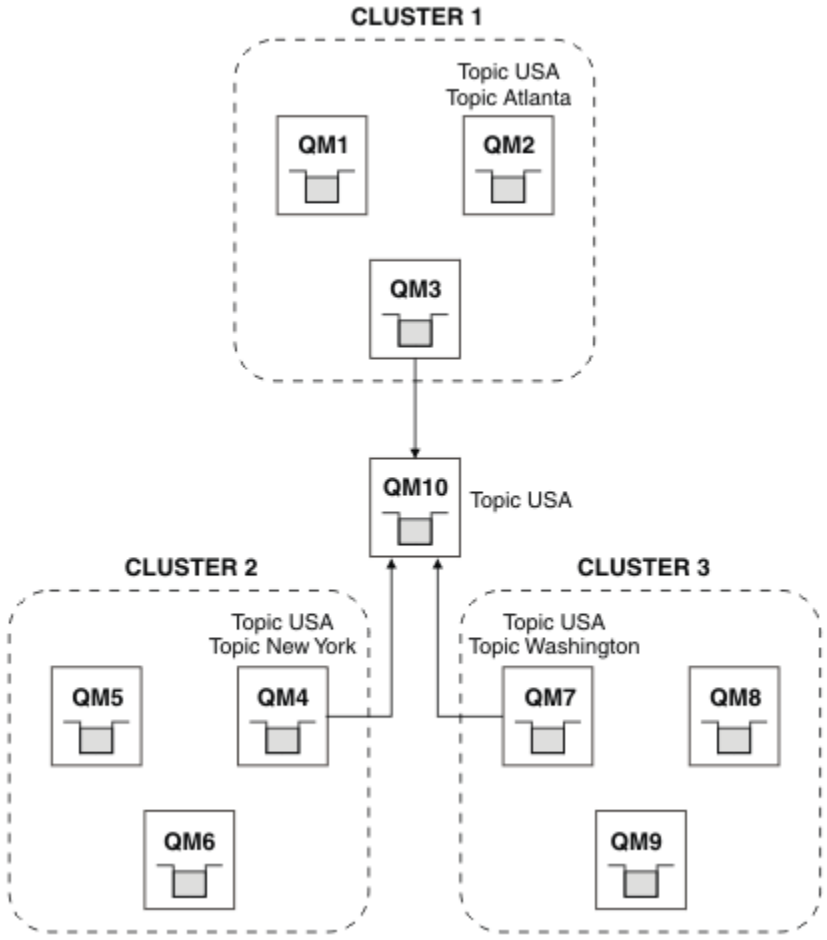
Než začnete

Prověřte téma “Sloučení prostorů témat u více klastrů” na stránce 396. Může to být dostačující pro vaše potřeby, aniž byste přidali dalšího správce front jako most.

Poznámka: Tuto úlohu lze provést pouze pomocí přímých směrovaných klastrů publikování/odběru. To nelze provést pomocí klastrů se směrováním hostitele tématu.

Informace o této úloze

Potenciální zlepšení topologie zobrazené v produktu Obrázek 67 na stránce 397 v produktu “Sloučení prostorů témat u více klastrů” na stránce 396 spočívá v izolaci témat klastru, která nejsou sdílena mezi všemi klastry. Izolovat klastry vytvořením přemosťovacího správce front, který není v žádném z klastrů; viz Obrázek 68 na stránce 399. Pomocí správce front pro přemostění můžete filtrovat, které publikace a odběry mohou přecházet z jednoho klastru do jiného.



Obrázek 68. Propojené klastry

Pomocí mostu určete témata klastru, která nechcete vystavit na základě mostu na ostatních klastrech. V produktu Obrázek 68 na stránce 399je USA téma klastru sdílené ve všech klastrech a produkty `Atlanta`, `New York` a `Washington` jsou témata klastru, která jsou sdílena pouze v jednom klastru.

Modelujte konfiguraci pomocí následující procedury:

Postup

1. Upravte všechny objekty tématu produktu `SYSTEM.BASE.TOPIC` tak, aby měly produkt **SUBSCOPE** (`QMGR`). a **PUBSCOPE** (`QMGR`) na všech správcích front.

   Žádná témata (ani témata klastru) se nešíří do jiných správců front, pokud jste explicitně nenastavoval **SUBSCOPE** (`ALL`). a **PUBSCOPE** (`ALL`) v tématu týkajícím se kořenového adresáře témat klastru.
2. Definujte témata na třech správcích front hostitele témat klastru, které chcete sdílet v každém klastru s atributy **CLUSTER** (*clustername*), **SUBSCOPE** (`ALL`). a **PUBSCOPE** (`ALL`).

   Chcete-li některá témata klastru sdílet mezi všemi klastry, definujte stejné téma v každém z klastrů. Jako atribut klastru použijte název klastru každého klastru.
3. V případě témat klastru, která chcete sdílet mezi všemi klastry, definujte témata znovu ve správci front mostu (`QM10`) s atributy **SUBSCOPE** (`ALL`) a **PUBSCOPE** (`ALL`).

Příklad

V příkladu v produktu Obrázek 68 na stránce 399se šíří pouze témata, která dědí od USA mezi všemi třemi klastry.

Jak pokračovat dále

Odběry pro témata definovaná ve správci front mostu s produktem **SUBSCOPE** (ALL) a **PUBSCOPE** (ALL) jsou šířeny mezi klastry.

Odběry pro témata definovaná v rámci každého klastru s atributy **CLUSTER** (*clustername*), **SUBSCOPE** (ALL) a **PUBSCOPE** (ALL) jsou šířeny v rámci každého klastru.

Všechny ostatní odběry jsou lokální pro správce front.

Související pojmy

Distribuované sítě typu publikování/odběr

Prostory tématu

Obor publikování

Obor odběru

Související úlohy

Vytvoření jediného prostoru tématu v klastru publikování/odběru
Rozšiřte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

Přidání správce front produktu IBM WebSphere MQ 7 nebo novější do existujících prostorů témat IBM WebSphere MQ 6
Rozšiřte existující systém publikování/odběru produktu IBM WebSphere MQ 6 tak, aby spolupracovat s produktem IBM WebSphere MQ 7 nebo novějším správcem front a sdílel stejné prostory témat.

Sloučení prostorů témat u více klastrů
Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Publikování a přihlášení k odběru prostorů témat ve více klastrech
Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Definování témat klastru

Publikování a přihlášení k odběru prostorů témat ve více klastrech

Publikování a odběr témat ve více klastrech pomocí překrývajících se klastrů. Tuto techniku můžete použít tak dlouho, dokud se prostory tématu v klastrech nepřekrývají.

Než začnete

Vytvořte více tradičních klastrů s některými správci front v průsečících mezi klastry.

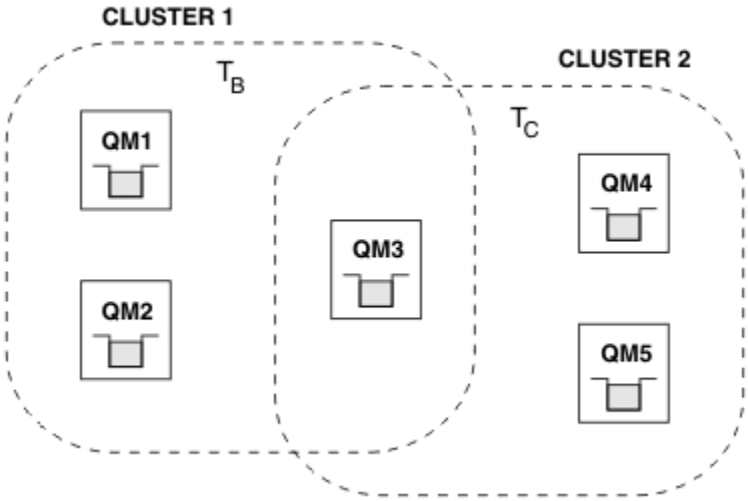
Informace o této úloze

Možná jste se rozhodli překrývat klastry pro různé různé důvody.

1. Máte omezený počet serverů s vysokou dostupností nebo správců front. Rozhodli jste se implementovat všechna úložiště klastru a hostitele klastru k nim.
2. Máte existující klastry tradičních správců front, které jsou připojeny pomocí správců front brány. Chcete implementovat aplikace publikování/odběru do stejné topologie klastru.
3. Máte několik samostatně obsažených aplikací typu publikování/odběr. Z výkonnostních důvodů je lepší udržovat malé a oddělené klastry publikování/odběru odděleně od tradičních klastrů. Rozhodli jste se implementovat aplikace do různých klastrů. Avšak také chcete monitorovat všechny aplikace publikování/odběru na jednom správci front, protože jste licencovali pouze jednu kopii aplikace monitorování. Tento správce front musí mít přístup k publikacím na témata klastru ve všech klastrech.

Tím, že zajistíte, aby vaše témata byla definována v nepřekrývaných prostorech témat, můžete implementovat témata do překrývajících se klastrů publikování/odběru, viz Obrázek 69 na stránce 401. Pokud se mezery tématu překrývají, pak implementace do překrývajících se klastrů bude mít za následek problémy.

Vzhledem k tomu, že klastry publikování/odběru se překrývají, můžete publikovat a odebírat kterýkoli z prostorů témat používajících správce front v překryvu.



Obrázek 69. Překrývající se klastry, nepřekrývající se prostory tématu

Postup

Vytvořte prostředek, který zajistí, aby se prostory tématu nepřekrývaly.

Například definujte jedinečné kořenové téma pro každý z prostorů témat. Témata týkající se klastru kořenových témat proveďte jako témata.

a) `DEFINE TOPIC(B) TOPICSTR('B') CLUSTER('CLUSTER 1') ...`

b) `DEFINE TOPIC(C) TOPICSTR('C') CLUSTER('CLUSTER 2') ...`

Příklad

V produktu Obrázek 69 na stránce 401 vydavatelé a odběratel, který je připojen k produktu `QM3` , může publikovat nebo odebírat T $_{B}$ nebo T $_{C}$

Jak pokračovat dále

Navázat vydavatele a odběratele, kteří používají témata v obou klastrech pro správce front v překryvu.

Připojte vydavatele a odběratele, kteří musí používat pouze témata ve specifickém klastru pro správce front, kteří nejsou v překryvu.

Související pojmy

Distribuované sítě typu publikování/odběr

Prostory tématu

Související úlohy

Vytvoření jediného prostoru tématu v klastru publikování/odběru
Rozšiřte systém publikování/odběru tak, aby se spouštěl na více správcích front. Klastr publikování/odběru použijte k poskytnutí každého vydavatele a odběratele s jedním identickým prostorem tématu.

Přidání správce front produktu IBM WebSphere MQ 7 nebo novější do existujících prostorů témat IBM WebSphere MQ 6
Rozšiřte existující systém publikování/odběru produktu IBM WebSphere MQ 6 tak, aby spolupracovat s produktem IBM WebSphere MQ 7 nebo novějším správcem front a sdílel stejné prostory témat.

Sloučení prostorů témat u více klastrů
Vytvořte prostory témat, které zahrnují více klastrů. Publikovat na téma v jednom klastru a přihlásit se k odběru v jiném klastru.

Kombinování a izolování prostorů témat ve více klastrech
Izolovat některé prostory témat do specifického klastru a kombinovat další prostory témat, aby byly přístupné ve všech připojených klastrech.

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 “Spouštění publikování/odběru ve frontě” na stránce 383.
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 288.
   - 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 technologie distribuovaných front” na stránce 172.

   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 sítí distribuovaných publikování/odběru” na stránce 386.

Související pojmy

Kombinování oborů publikování a odběrů

Počínaje produktem IBM WebSphere MQ 7.0 pracuje obor publikování a odběru prací nezávisle na určení toku publikování mezi správci front.

Kombinování prostorů témat v sítích typu publikování/odběr

Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Proudy a témata

Systém zpráv publikování/odběru

Související úlohy

Konfigurace klastru publikování/odběru

Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesun definice tématu klastru do jiného správce front

Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu

V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou 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

ZOBRAZIT PUBSUB

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

Kombinování oborů publikování a odběrů
Počínaje produktem IBM WebSphere MQ 7.0 pracuje obor publikování a odběru prací nezávisle na určení toku publikování mezi správci front.

Kombinování prostorů témat v sítích typu publikování/odběr
Zkombinujte prostor tématu správce front s ostatními správci front v klastru nebo v klastru publikování/odběru. Kombinování klastrů publikování/odběru a publikování/odběru klastrů s hierarchiemi.

Související úlohy

Konfigurace klastru publikování/odběru
Definujte téma ve správci front. Chcete-li vytvořit téma tématu klastru, nastavte vlastnost **CLUSTER** . Chcete-li zvolit směrování, které má být použito pro publikace a odběry pro toto téma, nastavte vlastnost **CLROUTE** .

Přesun definice tématu klastru do jiného správce front
Pro klastry routed nebo přímé směrované klastry může být zapotřebí při vyřazování správce front z provozu přesunout definici tématu klastru, nebo proto, že správce front klastru selhal nebo není k dispozici pro významné časové období.

Přidání dalších hostitelů témat do klastru se směrováním hostitele tématu
V klastru publikování/odběru se směrovaným hostitelem odběru lze více správců front použít k směrování publikování do odběrů definováním stejného objektu klastrovaného tématu u těchto správců front. To lze použít ke zlepšení dostupnosti a vyrovnávání pracovní zátěže. Pokud přidáte dalšího hostitele tématu pro stejný objekt tématu klastru, můžete použít parametr **PUB** k řízení toho, kdy se publikování začnou 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.

ULW Konfigurace více instalací

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

Informace o této úloze

Tyto informace platí pro UNIX, Linux, and Windows.

Procedura

- Při konfiguraci vašich instalací použijte informace v následujících odkazech:
  - “Změna primární instalace” na stránce 413
  - “Přidružení správce front k instalaci” na stránce 415
  - “Připojování aplikací v prostředí s více instalačními prostředí” na stránce 405

ULW Připojování aplikací v prostředí s více instalačními prostředí

On UNIX, Linux, and Windows systems, if IBM WebSphere MQ 7.1, or later, libraries are loaded, IBM MQ automatically uses the appropriate libraries without you needing to take any further action. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Následující koncepty se používají k vysvětlení způsobu připojení aplikací k produktu IBM MQ:

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

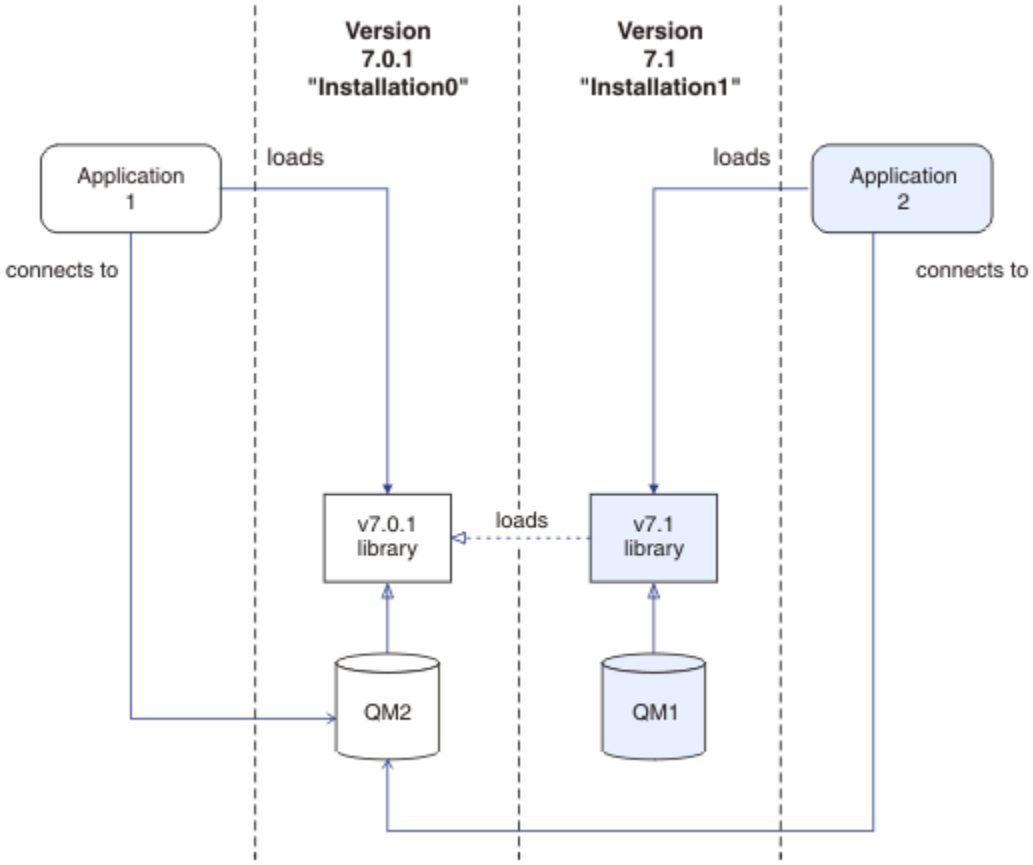
Zavádění
Když je aplikace spuštěna, jsou umístěny a zavedeny knihovny produktu IBM MQ . Specifický mechanismus použitý k vyhledání knihoven se liší podle operačního systému a podle toho, jak je aplikace sestavena. Další informace o tom, jak vyhledat a načíst knihovny ve více instalačních prostředích, najdete v tématu “Načítání knihoven produktu IBM MQ” na stránce 407.

Připojování
Když se aplikace připojí ke spuštěnému správci front, například pomocí volání `MQCONN` nebo `MQCONNX` , připojí se k použití načtených knihoven produktu IBM MQ .

Když se serverová aplikace připojuje ke správci front, musí načtené knihovny pocházet z instalace přidružené ke správci front. Při použití více instalací v systému toto omezení představuje nové problémy při výběru mechanizmu, který operační systém používá k vyhledání knihoven produktu IBM MQ , které mají být načteny:

- Pokud se příkaz **setmqm** používá ke změně instalace přidružené ke správci front, knihovny, které je třeba načíst, se mění.
- Když se aplikace připojuje k více správcům front, kteří jsou vlastněny různými instalacemi, musí být načteno více sad knihoven.

Nicméně, pokud je IBM WebSphere MQ 7.1nebo pozdější knihovny, jsou umístěny a zavedeny, IBM MQ pak zavede a použije příslušné knihovny, aniž byste potřebovali provést další akce. Když se aplikace připojí ke správci front, produkt IBM MQ načte knihovny z instalace, ke které je přidružen správce front.



Obrázek 70. Připojování aplikací v prostředí s více instalačními prostředí

Například Obrázek 70 na stránce 406 ukazuje vícenásobné instalační prostředí s instalací IBM WebSphere MQ 7.0.1 (`Installation0`) a instalací IBM WebSphere MQ 7.1 (`Installation1`). K těmto instalacím jsou připojeny dvě aplikace, ale načítají různé verze knihoven.

Produkt `Application 1` přímo načte knihovnu IBM WebSphere MQ 7.0.1 . Když se produkt `application 1` připojí k produktu `QM2`, použijí se knihovny IBM WebSphere MQ 7.0.1 . Pokud se produkt `application 1` pokusí o připojení k produktu `QM1`nebo pokud je `QM2` přidružen k produktu `Installation1`, dojde k selhání `application 1` s chybou 2059 (080B) (RC2059): MQRC_Q_MGR_NOT_AVAILABLE . Aplikace selže, protože knihovna IBM WebSphere MQ 7.0.1 není schopna načíst jiné verze knihovny. To znamená, že pokud jsou knihovny IBM WebSphere MQ 7.0.1 přímo načteny, nelze k instalaci použít správce front přidruženého k instalaci v novější verzi produktu IBM MQ.

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

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

Další informace o způsobu načítání knihoven produktu IBM WebSphere MQ 7.1 naleznete v tématu “Načítání knihoven produktu IBM MQ” na stránce 407.

Podpora a omezení

Pokud jsou umístěny a načteny některé z následujících knihoven IBM WebSphere MQ 7.1nebo novější, může produkt IBM MQ automaticky načíst a použít příslušné knihovny:

- Knihovny serveru jazyka C
- Knihovny serveru C++
- Knihovny serveru XA
- Knihovny serveru COBOL
- Knihovny serveru COM +
- .NET v nespravovaném režimu

Produkt IBM MQ také automaticky načítá a používá příslušné knihovny pro aplikace Java a JMS v režimu vazeb.

Pro aplikace používající více instalací existuje několik omezení. Další informace viz “Omezení pro aplikace používající více instalací” na stránce 410.

Související pojmy

“Omezení pro aplikace používající více instalací” na stránce 410
Existují omezení při použití knihoven serveru produktu CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními podmínkami.

“Načítání knihoven produktu IBM MQ” na stránce 407
Při rozhodování o načtení knihoven produktu IBM MQ je třeba zvážit řadu faktorů, včetně: vašeho prostředí, zda můžete změnit existující aplikace, zda chcete primární instalaci, kde je nainstalován produkt IBM MQ a zda se bude umístění produktu IBM MQ pravděpodobně měnit.

Související úlohy

Výběr primární instalace

“Změna primární instalace” na stránce 413
K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz **setmqinst** .

“Přidružení správce front k instalaci” na stránce 415
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému UNIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

ULW Načítání knihoven produktu IBM MQ

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

Tyto informace platí pro verzi produktu IBM WebSphere MQ 7.1nebo novější knihovny.

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

- Je-li v systému UNIX and Linux nainstalována kopie produktu IBM WebSphere MQ 7.1nebo novější verze ve výchozím umístění, stávající aplikace budou nadále pracovat stejným způsobem jako předchozí verze. Pokud však aplikace potřebují symbolické odkazy v produktu `/usr/lib`, musíte buď vybrat instalaci produktu IBM WebSphere MQ 7.1nebo pozdější verzi, instalaci jako primární instalaci, nebo ručně vytvořit symbolické odkazy.
- Je-li produkt IBM WebSphere MQ 7.1nebo novější verze nainstalován v jiném než výchozím umístění, což je případ, kdy je nainstalován také produkt IBM WebSphere MQ 7.0.1 , může být zapotřebí změnit existující aplikace tak, aby byly načteny správné knihovny.

Způsob umístění a načítání knihoven produktu IBM MQ závisí také na tom, jak jsou nastaveny všechny existující aplikace k načtení knihoven. Další informace o tom, jak lze načíst knihovny, najdete v tématu “Mechanismy zavádění knihoven operačního systému” na stránce 409.

Optimálně byste měli zajistit, aby knihovna IBM MQ , která je zavedena operačním systémem, byla přidružena k tomuto správci front.

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

Tabulka 29. Výhody a nevýhody voleb pro načítání knihoven

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

Tabulka 29. Výhody a nevýhody voleb pro načítání knihoven (pokračování)

Platforma	Volba	Výhody	Nevýhody
ULW UNIX, Linux, and Windows systémy	Nastavte primární instalaci na server IBM WebSphere MQ 7.1nebo novější, instalaci. Viz “Změna primární instalace” na stránce 413. 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.	• Je-li nainstalován produkt IBM WebSphere MQ 7.0.1 , nelze primární instalaci nastavit na verzi IBM WebSphere MQ 7.1nebo novější. • Linux UNIX UNIX and Linux: Nefunguje, pokud `/usr/lib` není ve výchozí vyhledávací cestě.

Aspekty implementace knihovny pro produkt Linux

Linux

Aplikace kompilované pomocí některých verzí gcc, například, verze 3.2.x, mohou mít vestavěnou cestu RPath, kterou nelze přepsat pomocí proměnné prostředí *LD_LIBRARY_PATH* . Pomocí příkazu `readelf -d` *`applicationName`* můžete určit, zda je aplikace ovlivněna. Cestu RPath nelze přepsat, je-li přítomen symbol RPATH a že není přítomen symbol RUNPATH.

Aspekty implementace knihovny pro produkt Solaris

Solaris

Ukázkové příkazy kompilace v dokumentaci produktu pro předchozí verze produktu IBM MQ obsahovaly volby propojení `-lmqmcs -lmqmzse` . Odpovídající verze těchto knihoven jsou nyní načíteny automaticky produktem IBM MQ. Je-li produkt IBM MQ nainstalován v jiném než výchozím umístění, nebo pokud v systému existuje více instalací, je třeba aktualizovat aplikace. Aplikace můžete aktualizovat opětovným kompilováním a propojením bez voleb odkazu `-lmqmcs -lmqmzse` .

Mechanismy zavádění knihoven operačního systému

Na systémech Windows se prohledají několik adresářů, kde najdete knihovny:

- Adresář, ze kterého je aplikace načtena.
- Aktuální adresář.
- Adresáře v proměnné prostředí *PATH* , jak globální proměnná *PATH* , tak i proměnná *PATH* aktuálního uživatele.

Linux UNIX V systémech UNIX and Linux existuje řada metod, které mohly být použity k vyhledání knihoven k načtení:

- Pomocí proměnné prostředí *LD_LIBRARY_PATH* (také *LIBPATH* na AIX). Je-li tato proměnná nastavena, definuje sadu adresářů, které se prohledají pro požadované knihovny IBM MQ . Pokud jsou v těchto adresářích nalezeny nějaké knihovny, používají se v předvolbách všech knihoven, které by mohly být nalezeny pomocí jiných metod.
- Použití vestavěné vyhledávací cesty (RPath). Aplikace může obsahovat sadu adresářů, které se mají prohledávat kvůli knihovnám IBM MQ . Pokud není proměnná *LD_LIBRARY_PATH* nastavena, nebo pokud požadované knihovny nebyly nalezeny pomocí proměnné, prohledá se cesta RPath pro knihovny. Pokud vaše existující aplikace používají RPath, ale aplikaci nemůžete překompilovat a propojit, musíte

buď nainstalovat produkt IBM WebSphere MQ 7.1 do výchozího umístění, nebo použít jinou metodu k vyhledání knihoven.

- Použije se výchozí cesta ke knihovně. Pokud se knihovny produktu IBM MQ nenaleznou po prohledání proměnné *LD_LIBRARY_PATH* a umístění RPath, prohledá se výchozí cesta ke knihovně. Tato cesta obvykle obsahuje `/usr/lib` nebo `/usr/lib64`. Nejsou-li knihovny nalezeny po prohledání předvolené cesty ke knihovně, spuštění aplikace se nezdaří kvůli chybějícím závislostem.

Můžete použít mechanizmus operačního systému, abyste zjistili, zda vaše aplikace mají vestavěnou vyhledávací cestu. Příklad:

- AIX: **dump**
- Linux: **readelf**
- Solaris: **elfdump**

Související pojmy

"Omezení pro aplikace používající více instalací" na stránce 410
Existují omezení při použití knihoven serveru produktu CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními podmínkami.

"Připojování aplikací v prostředí s více instalačními prostředí" na stránce 405
On UNIX, Linux, and Windows systems, if IBM WebSphere MQ 7.1, or later, libraries are loaded, IBM MQ automatically uses the appropriate libraries without you needing to take any further action. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Související úlohy

Výběr primární instalace

"Změna primární instalace" na stránce 413
K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz **setmqinst** .

"Přidružení správce front k instalaci" na stránce 415
Když vytvoříte správce front, je automaticky přidružen k instalaci, která vydala příkaz **crtmqm** . V systému UNIX, Linux, and Windowsmůžete změnit instalaci přidruženou ke správci front pomocí příkazu **setmqm** .

ULW Omezení pro aplikace používající více instalací

Existují omezení při použití knihoven serveru produktu CICS , připojení rychlých cest, obslužných rutin zpráv a uživatelských procedur v prostředí s více instalačními podmínkami.

Knihovny serveru CICS

Používáte-li knihovny serveru CICS , produkt IBM MQ pro vás automaticky nevybere správnou úroveň knihovny. Musíte zkompilovat a propojit aplikace s příslušnou úrovní knihovny pro správce front, ke kterému se aplikace připojuje. Další informace naleznete v tématu Sestavování knihoven pro použití s produktem TXSeries for Multiplatforms verze 5.

Obslužné rutiny zpráv

Popisovače zpráv, které používají speciální hodnotu `MQHC_UNASSOCIATED_HCONN` , jsou omezeny na použití při první instalaci načtené do procesu. Pokud obslužnou rutinu zpráv nemůže použít konkrétní instalace, je vrácen kód příčiny `MQRC_HMSG_NOT_AVAILABLE` .

Toto omezení ovlivňuje vlastnosti zprávy. Obslužné rutiny zpráv nelze použít k získání vlastností zprávy od správce front v rámci jedné instalace a jejich umístění do správce front v jiné instalaci. Další informace o obslužných rutin zpráv naleznete v tématu MQCRTMH-Create message handle.

Uživatelské procedury

V prostředí s více instalacemi musí být existující uživatelské procedury aktualizovány pro použití s instalacemi produktu IBM WebSphere MQ 7.1nebo novější. Uživatelské procedury pro převod dat vygenerované pomocí příkazu **crtmqcvx** musí být znovu generovány s použitím aktualizovaného příkazu.

Všechny uživatelské procedury musí být zapsány pomocí struktury MQIEP , nelze použít vestavěný RPATH k vyhledání knihoven produktu IBM MQ a nemohou se odkazovat na knihovny IBM MQ . Další informace najdete v tématu Psaní výstupních vstupů a instalovatelných služeb na serveru UNIX, Linux, and Windows .

Rychlý způsob

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

1. Správce front musí být přidružen ke stejné instalaci jako ten, ze kterého aplikace načetla běhové knihovny IBM 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 jinak než rychlým způsobem ke správci front přidruženému k instalaci IBM WebSphere MQ 7.1 nebo novější nemá žádný vliv na to, zda se aplikace může připojit rychlým způsobem.
4. Nelze kombinovat připojení ke správci front přidruženému k instalaci produktu IBM WebSphere MQ 7.0.1 a připojení rychlé cesty ke správci front přidruženému k instalaci produktu IBM WebSphere MQ 7.1nebo novější.

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

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

Související odkazy

MQCONNX-Připojit správce front (rozšířený)
Struktura MQIEP
2583 (0A17) (RC2583): Rozhraní MQRC_INSTALLATION_MISMATCH
2587 (0A1B) (RC2587): MQRC_HMSG_NOT_AVAILABLE
2590 (0A1E) (RC2590): MQRC_FASTPATH_NOT_AVAILABLE

ULW Připojení aplikací produktu .NET v prostředí s více instalačními prostředí

Při výchozím nastavení aplikace používají montážní celky .NET z primární instalace. Pokud neexistuje žádná primární instalace, nebo nechcete použít žádné primární montážní celky, musíte aktualizovat konfigurační soubor aplikace nebo proměnnou prostředí *DEVPATH* .

Je-li v systému primární instalace, jsou soubory .NET a soubory zásad této instalace zaregistrovány do globální mezipaměti sestavení (GAC). Sestavy .NET pro všechny ostatní instalace lze najít v instalační cestě každé instalace, ale sestavy nejsou registrovány v GAC. Proto se aplikace standardně spouštějí s použitím montážních celků .NET z primární instalace. Konfigurační soubor aplikace je třeba aktualizovat, je-li splněna některá z následujících podmínek:

- Nemáte primární instalaci.
- Nechcete, aby aplikace používala montážní celky primárních instalací.
- Primární instalace je nižší verzí produktu IBM MQ než verze, se kterou byla aplikace zkompilována.

Informace o tom, jak aktualizovat konfigurační soubor aplikací, viz "Připojení aplikací produktu .NET s použitím konfiguračního souboru aplikace" na stránce 412.

Proměnnou prostředí *DEVPATH* je třeba aktualizovat, je-li splněna následující podmínka:

- Chcete, aby aplikace používala sestavy z jiné než primární instalace, ale primární instalace je na stejné verzi jako neprimární instalace.

Další informace o tom, jak aktualizovat proměnnou *DEVPATH* viz "Připojení aplikací .NET pomocí DEVPATH" na stránce 413.

Připojení aplikací produktu .NET s použitím konfiguračního souboru aplikace

V konfiguračním souboru aplikace je třeba nastavit různé značky pro přesměrování aplikací tak, aby používaly sestavy, které nejsou z primární instalace.

V následující tabulce jsou uvedeny specifické změny, které je třeba provést v konfiguračním souboru aplikací, aby se aplikace .NET připojily pomocí konkrétních sestav:

Tabulka 30. Konfigurace aplikací pro použití konkrétních sestav

	Aplikace kompilované se starší verzí produktu IBM MQ	**Aplikace kompilované s novější verzí produktu IBM MQ**
Chcete-li spustit aplikaci s vyšší verzí produktu IBM MQ , primární instalací. (novější verze sestav v GAC):	Nejsou nutné žádné změny	Nejsou nutné žádné změny
Chcete-li spustit aplikaci se starší verzí produktu IBM MQ , primární instalací. (předchozí sestavy verzí v GAC):	Nejsou nutné žádné změny	V konfiguračním souboru aplikace: • Použijte značku *bindingRedirect* k označení použití dřívější verze sestav, které jsou v GAC.
Chcete-li spustit aplikaci s novější verzí produktu IBM MQ , která není primární, použijte jinou než primární instalaci. (novější verze sestav v instalační složce):	V konfiguračním souboru aplikace: • Použijte značku *codebase* k určení umístění dalších montážních celků verzí • Použijte značku *bindingRedirect* k označení použití sestav pozdějších verzí	V konfiguračním souboru aplikace: • Použijte značku *codebase* k určení umístění dalších montážních celků verzí

Tabulka 30. Konfigurace aplikací pro použití konkrétních sestav (pokračování)		
	Aplikace kompilované se starší verzí produktu IBM MQ	**Aplikace kompilované s novější verzí produktu IBM MQ**
Chcete-li spustit aplikaci se starší verzí produktu IBM MQ , než je primární instalace. (předchozí sestavy verzí v instalační složce):	V konfiguračním souboru aplikace: • Použijte značku *codebase* k určení umístění sestav starších verzí • Zahrnout značku *publisherpolicy Apply=no*	V konfiguračním souboru aplikace: • Použijte značku *codebase* k určení umístění sestav starších verzí • Použijte značku *bindingRedirect* k označení použití sestav předchozí 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 může být upraven pomocí instalační cesty produktu IBM MQ jakékoli jiné než primární instalace. Soubor může být také přímo zahrnut do jiných konfiguračních souborů pomocí značky *linkedConfiguration* . Ukázky jsou k dispozici pro produkty `nmqsget.exe.config` a `nmqsput.exe.config`. Oba ukázky používají značku *linkedConfiguration* a obsahují soubor `NonPrimaryRedirect.config` .

Připojení aplikací .NET pomocí DEVPATH

Sestavy můžete najít pomocí proměnné prostředí *DEVPATH* . Sestavy uvedené v proměnné *DEVPATH* se používají jako předvolba pro všechny sestavy v GAC. Další informace o tom, kdy použít tuto proměnnou, najdete v příslušné dokumentaci produktu Microsoft v souboru *DEVPATH* .

Chcete-li vyhledat sestavy pomocí proměnné prostředí *DEVPATH* , musíte nastavit proměnnou *DEVPATH* na složku, která obsahuje sestavy, které chcete použít. Poté je třeba aktualizovat konfigurační soubor aplikace a přidat následující informace o konfiguraci běhového prostředí:

```
<configuration>
<runtime>
<developmentMode developerInstallation="true" />
</runtime>
</configuration>
```

Související pojmy

“Připojování aplikací v prostředí s více instalačními prostředí” na stránce 405
On UNIX, Linux, and Windows systems, if IBM WebSphere MQ 7.1, or later, libraries are loaded, IBM MQ automatically uses the appropriate libraries without you needing to take any further action. Produkt IBM MQ používá knihovny z instalace přidružené ke správci front, ke kterému se aplikace připojuje.

Více instalací

Související úlohy

Výběr primární instalace

Použití produktu .NET

ULW Změna primární instalace

K nastavení nebo zrušení nastavení instalace jako primární instalace můžete použít příkaz **setmqinst** .

Informace o této úloze

Tato úloha se týká produktu UNIX, Linux, and Windows.

Primární instalace je instalace, na kterou se odkazují požadované umístění v celém systému. Další informace o primární instalaci a pokyny k výběru primární instalace naleznete v tématu Výběr primární instalace.

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

Windows Během procesu instalace v systému Windowsmůžete určit, že se má instalace primární instalací.

Linux UNIX Na systémech UNIX and Linux musíte po instalaci zadat příkaz **setmqinst** , který nastaví instalaci jako primární instalaci.

Procedura

- Chcete-li nastavit instalaci jako primární instalaci, proveďte následující kroky:
  a) Zkontrolujte, zda je instalace již primární instalací, zadáním následujícího příkazu:

     ```
     MQ_INSTALLATION_PATH/bin/dspmqinst
     ```

     kde *MQ_INSTALLATION_PATH* je instalační cesta k instalaci produktu IBM WebSphere MQ 7.1 nebo pozdější.
  b) Je-li existující instalace produktu IBM WebSphere MQ 7.1 nebo novější nastavena jako primární instalace, unset it před pokračováním s dalším krokem.

     Je-li v systému nainstalován produkt IBM WebSphere MQ 7.0.1 , nelze primární instalaci změnit.
  c) Ujistěte se, že jste přihlášeni s příslušným oprávněním:
     – UNIX Jako uživatel root v systému UNIX and Linux.
     – Linux Jako člen skupiny administrátorů na systémech Windows .
  d) Zadejte jeden z následujících příkazů:
     – Chcete-li nastavit primární instalaci pomocí cesty k instalaci, kterou chcete použít jako primární instalaci, postupujte takto:

       ```
       MQ_INSTALLATION_PATH/bin/setmqinst -i -p MQ_INSTALLATION_PATH
       ```

     – Chcete-li nastavit primární instalaci pomocí názvu instalace, kterou chcete provést jako primární, postupujte takto:

       ```
       MQ_INSTALLATION_PATH/bin/setmqinst -i -n installationName
       ```

  e) Windows
     V systémech Windows restartujte systém.
- Chcete-li zrušit nastavení instalace jako primární instalace, proveďte následující kroky:
  a) Zkontrolujte, která instalace je primární instalací, zadáním následujícího příkazu:

     ```
     MQ_INSTALLATION_PATH/bin/dspmqinst
     ```

     kde *MQ_INSTALLATION_PATH* je instalační cesta k instalaci produktu IBM WebSphere MQ 7.1 nebo pozdější.

     Je-li IBM WebSphere MQ 7.0.1 primární instalací, nemůžete zrušit nastavení primární instalace.

b) Ujistěte se, že jste přihlášeni s příslušným oprávněním:

- UNIX Jako uživatel root v systému UNIX and Linux.
- Linux Jako člen skupiny administrátorů na systémech Windows .

c) Zadejte jeden z následujících příkazů:

- Chcete-li zrušit nastavení primární instalace pomocí cesty k instalaci, již nadále nechcete být primární instalací, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -x -p MQ_INSTALLATION_PATH
```

- Chcete-li zrušit nastavení primární instalace s použitím názvu instalace, již nadále nechcete být primární instalací, postupujte takto:

```
MQ_INSTALLATION_PATH/bin/setmqinst -x -n installationName
```

Související pojmy

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

Odkazy na externí knihovny a řídicí příkaz pro primární instalaci v systému UNIX and Linux

Související úlohy

Odinstalování, upgrade a údržba primární instalace

Výběr názvu instalace

Související odkazy

setmqinst

ULW Přidružení správce front k instalaci

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

Informace o této úloze

Instalace, ke které je správce front přidružen, omezuje správce front tak, aby mohl být spravován pouze příkazy z této instalace. Existují tři klíčové výjimky:

- Volba **setmqm** změní instalaci přidruženou ke správci front. Tento příkaz musí být zadán z instalace, kterou chcete přidružit ke správci front, nikoli k instalaci, k níž je aktuálně přidružen správce front. Název instalace zadaný příkazem **setmqm** musí odpovídat instalaci, ze které se příkaz vydal.
- Volba **strmqm** obvykle musí být vydána z instalace, která je přidružena ke správci front. Je-li však správce front IBM WebSphere MQ 7.0.1 nebo dřívější spuštěn v systému IBM WebSphere MQ 7.1 nebo pozdější instalaci poprvé, lze použít příkaz **strmqm** . V takovém případě produkt **strmqm** spustí správce front a přidruží jej k instalaci, ze které je příkaz zadán.
- Volba **dspmq** zobrazí informace o všech správcích front v systému, nikoli pouze o těch správcích front přidružených ke stejné instalaci jako příkaz **dspmq** . Příkaz `dspmq -o installation` zobrazí informace o tom, které správci front jsou přidruženi k instalacím.

Pro prostředí HA příkaz **addmqinf** automaticky asociuje správce front s instalací, ze které je příkaz **addmqinf** zadán. Pokud je příkaz **strmqm** zadán ze stejné instalace jako příkaz **addmqinf** , není třeba žádné další nastavení. Chcete-li spustit správce front pomocí jiné instalace, je třeba nejprve změnit přidruženou instalaci pomocí příkazu **setmqm** .

Chcete-li přidružit správce front k instalaci, můžete použít příkaz **setmqm** následujícími způsoby:

- Přesun jednotlivých správců front mezi rovnocennými verzemi produktu IBM MQ. Například přesun správce front z testovacího do produkčního systému.

- Migrace jednotlivých správců front ze starší verze produktu IBM MQ na novější verzi produktu IBM MQ. Migrace správců front mezi verzemi má různé důsledky, o kterých si musíte být vědomi. Další informace o migraci naleznete v tématu Údržba a migrace.

Postup

1. Zastavte správce front pomocí příkazu **endmqm** z instalace, která je aktuálně asociována se správcem front.
2. Přidružte správce front k jiné instalaci pomocí příkazu **setmqm** z této instalace.

   Chcete-li například nastavit správce front QMB tak, aby byl přidružen k instalaci s názvem Installation2, zadejte do adresáře Installation2: tento příkaz:

   ```
   MQ_INSTALLATION_PATH/bin/setmqm -m QMB -n Installation2
   ```

   kde *MQ_INSTALLATION_PATH* je cesta, kde je nainstalována Installation2 .
3. Spusťte správce front pomocí příkazu **strmqm** z instalace, která je nyní přidružena ke správci front.

   Tento příkaz provede nezbytnou migraci správce front a jeho výsledky budou připraveny k použití správcem front.

Jak pokračovat dále

Je-li instalace, ke které je přidružen správce front, odstraněna, nebo pokud jsou informace o stavu správce front nedostupné, příkaz **setmqm** nepřidružuje správce front k jiné instalaci. V této situaci proveďte následující akce:

1. Použijte příkaz **dspmqinst** , abyste viděli ostatní instalace na vašem systému.
2. Ručně upravte pole InstallationName oddílu QueueManager v souboru mqs.ini tak, aby určoval jinou instalaci.
3. K odstranění správce front použijte příkaz **dltmqm** z této instalace.

Související pojmy

“Vyhledání instalací produktu IBM MQ v systému” na stránce 416
Máte-li v systému více instalací produktu IBM MQ , můžete zkontrolovat, které verze jsou nainstalované a kde jsou.

“IBM MQ konfigurační soubor mqs.ini” na stránce 82
Konfigurační soubor IBM MQ mqs.iniobsahuje informace důležité pro všechny správce front v uzlu. Vytvoří se automaticky během instalace.

Související úlohy

Výběr primární instalace

Související odkazy

addmqinf
dspmq
dspmqinst
endmqm
setmqm
strmqm

ULW Vyhledání instalací produktu IBM MQ v systému

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

Při hledání instalací produktu IBM MQ ve vašem systému můžete použít následující metody:

- Použijte příkaz **dspmqver** . Tento příkaz neposkytuje podrobné informace o všech instalacích v systému, pokud je tento příkaz vydán z instalace produktu IBM WebSphere MQ 7.0.1 .
- Použijte instalační nástroje platformy pro dotaz, kde byl nainstalován produkt IBM MQ . Potom použijte příkaz **dspmqver** z instalace produktu IBM WebSphere MQ 7.1 nebo novější. Následující příkazy jsou příklady příkazů, které můžete použít k dotazování tam, kde byl nainstalován produkt IBM MQ :
  - AIX V systémech AIX můžete použít příkaz **lslpp** :

    ```
    lslpp -R ALL -l mqm.base.runtime
    ```

  - Linux V systémech Linux můžete použít příkaz **rpm** :

    ```
    rpm -qa --qf "%{NAME}-%{VERSION}-%{RELEASE}\t%{INSTPREFIXES}\n" | grep MQSeriesRuntime
    ```

  - Solaris V systémech Solaris můžete použít příkazy **pkginfo** a **pkgparam** :
    1. Seznam instalovaných balíků lze vypsat zadáním následujícího příkazu:

       ```
       pkginfo | grep -w mqm
       ```

    2. Pro každý vypsaný balík zadejte následující příkaz:

       ```
       pkgparam pkgname BASEDIR
       ```

  - Windows V systémech Windows můžete použít příkaz **wmic** . Tento příkaz může instalovat klienta wmic:

    ```
    wmic product where "(Name like '%MQ%') AND (not Name like '%bitSupport')" get Name,
    Version, InstallLocation
    ```

- Linux UNIX Na systémech UNIX and Linux zadejte následující příkaz, abyste zjistili, kde je nainstalován produkt IBM MQ :

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

  Potom použijte příkaz **dspmqver** z instalace produktu IBM WebSphere MQ 7.1 nebo novější.
- Windows Chcete-li zobrazit podrobnosti o instalacích na systému na 32bitovém systému Windows, zadejte následující příkaz:

  ```
  reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\IBM\WebSphere MQ\Installation" /s
  ```

- Windows V 64bitovém systému Windowszadejte následující příkaz:

  ```
  reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\IBM\WebSphere MQ\Installation" /s
  ```

Příkaz **reg.exe** zobrazuje pouze informace pro instalaci produktu IBM WebSphere MQ 7.1 nebo pozdější.

Související pojmy
Více instalací
Související odkazy
dspmqver
dspmqinst

Konfigurace vysoké dostupnosti, zotavení a restartu

V případě selhání správce front a zotavováním zpráv po selhání serveru nebo paměti můžete zajistit dostupnost aplikací s vysokou dostupností.

Informace o této úloze

z/OS V systému z/OSje vysoká dostupnost vestavěna do platformy. Také můžete zlepšit dostupnost serverové aplikace pomocí skupin sdílení front. Viz Sdílené fronty a skupiny sdílení front.

Multi V systému Multiplatformsmůžete zvýšit dostupnost klientských aplikací pomocí opětovného připojení klienta k automatickému přepnutí klienta mezi skupinou správců front nebo novou aktivní instancí správce front s více instancemi po selhání správce front. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů. Správce front pro více instancí je konfigurován tak, aby se spouštěl jako jeden správce front na více serverech. Implementujete aplikace serveru do tohoto správce front. Dojde-li k selhání serveru, na kterém je spuštěna aktivní instance, je provedení automaticky přepnuto na instanci v pohotovostním režimu téhož správce front na jiném serveru. Pokud nakonfigurujete serverové aplikace tak, aby se spouštěly jako služby správce front, restartují se, když se rezervní instance stane aktivně spuštěnou instancí správce front.

Dalším způsobem, jak zvýšit dostupnost serverové aplikace na platformách Multiplatforms, je implementovat serverové aplikace na více počítačů v klastru správců front. Počínaje produktem IBM WebSphere MQ 7.1 operace zotavení z chyb klastru spouští operace, které způsobily problémy, dokud nejsou vyřešeny problémy. Viz Změny na zotavení z chyb klastru na serverech jiných než z/OS. Produkt IBM MQ for Multiplatforms můžete také nakonfigurovat jako součást klastrového řešení specifického pro platformu, jako např.:

- Microsoft Klastrovaný server
- IBM i Klastry HA na systému IBM i
- Linux UNIX PowerHA pro AIX (dříve HACMP na AIX) a další řešení klastrování UNIX and Linux

Linux V systému Linux můžete nakonfigurovat replikované správce datových front (RQMs) k implementaci řešení vysoké dostupnosti nebo zotavení z havárie. V případě vysoké dostupnosti jsou instance stejného správce front konfigurovány na každém uzlu ve skupině tří serverů Linux . Jedna ze tří instancí je aktivní instance. Data z aktivního správce front jsou synchronně replikována do ostatních dvou instancí, takže jedna z těchto instancí může v případě nějakého selhání převzít. V případě zotavení z havárie je správce front spuštěn v primárním uzlu na jednom serveru se sekundární instancí tohoto správce front umístěného na uzlu zotavení na jiném serveru. Data se replikují mezi primární instancí a sekundární instancí, a pokud je primární uzel z nějakého důvodu ztracen, sekundární instanci může být provedena do primární instance a spuštěna.

MQ Appliance Další možností řešení vysoké dostupnosti nebo zotavení z havárie je implementovat pár zařízení produktu IBM MQ . Viz High Availability a Disaster Recovery v dokumentaci produktu IBM MQ Appliance .

Systém zasílání zpráv zajišťuje, že zprávy zadané do systému budou doručeny do místa určení. Produkt IBM MQ může trasovat přenosovou cestu ke zprávě při přesunu z jednoho správce front do jiného pomocí příkazu **dspmqrte** . Dojde-li k selhání systému, mohou být zprávy obnoveny různými způsoby v závislosti na typu selhání a způsobu, jakým je systém nakonfigurován. Produkt IBM MQ uchovává protokoly o zotavení aktivit správců front, kteří zpracovávají zprávy o příjmu, přenosu a doručování zpráv.Využívá tyto protokoly pro tři typy obnovy:

1. *Restartovat obnovu*, když zastavujete IBM MQ v plánovaném způsobu.
2. *Zotavení po selhání*, pokud se selhání zastaví IBM MQ.
3. *Obnova médií*, chcete-li obnovit poškozené objekty.

Ve všech případech obnova obnoví správce front do stavu, v němž se nacházela při zastavení správce front s tím rozdílem, že všechny transakce v době letu byly odvolány a odebrány z front všechny aktualizace, které byly v době zastavení správce front k dispozici v době zastavení. Obnova obnoví všechny trvalé zprávy, přechodné zprávy mohou být během procesu ztraceny.

POZOR: Protokoly pro zotavení nelze přesouvat do jiného operačního systému.

Automatické opětovné připojení klienta

Můžete provést automatické opětovné připojení klientských aplikací, aniž byste zapisoval nějaký dodatečný kód, a to konfigurací počtu komponent.

Automatické opětovné připojení klienta je *vložené*. Toto připojení se automaticky obnoví v každém okamžiku aplikačního programu klienta a obnoví se všechny popisovače k otevřeným objektům.

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 31 na stránce 420 uvádí nejstarší vydání podpory klienta IBM MQ , které musí být nainstalováno na pracovní stanici klienta. Pracovní stanice klienta je třeba převést na jednu z těchto úrovní pro aplikaci, která má používat automatické opětovné připojení klienta. Tabulka 32 na stránce 420 vypíše další požadavky, které umožní automatické opětovné připojení klienta.

Při přístupu programu k volbám opětovného připojení může klientská aplikace nastavit možnosti opětovného připojení. S výjimkou klientů JMS a XMS , má-li klientská aplikace přístup k volbám opětovného připojení, může také vytvořit obslužnou rutinu událostí pro obsluhu událostí opětovného připojení.

Existující klientská aplikace může mít prospěch z podpory opětovného připojení, bez rekompilace a linkování:

- V případě klienta jiného typu nežJMS nastavte proměnnou prostředí `mqclient.ini` `DefRecon` na nastavení možností opětného připojení. Použijte tabulku CCDT pro připojení ke správci front. Pokud se má klient připojit ke správci front s více instancemi, zadejte síťové adresy aktivních a rezervních instancí správce front v tabulce CCDT. Pro replikovaného správce datových front nebo správce front HA na serveru IBM MQ můžete zadat plovoucí adresu IP používanou aktivními i záložními správci front pro zjednodušení konfigurace.
- Pro klienta produktu JMS nastavte volby opětného připojení v konfiguraci továrny připojení. Při spuštění v kontejneru EJB serveru Java EE se objekty MDB mohou znovu připojit k produktu IBM MQ pomocí mechanismu opětného připojení poskytovaného aktivačními specifikacemi adaptéru prostředků produktu IBM MQ (nebo portů modulu listener, jsou-li spuštěny v produktu WebSphere Application Server). Pokud však aplikace není MDB (nebo je spuštěna ve webovém kontejneru), aplikace musí implementovat svou vlastní logiku opětovného připojení, protože automatické opětovné připojení klienta není v tomto scénáři podporováno. Adaptér prostředků produktu IBM MQ poskytuje tuto schopnost opětovného připojení pro doručování zpráv do objektů typu message-driven bean, ale jiné prvky produktu Java EE , jako jsou servlety, musí implementovat vlastní opětovné připojení.

Poznámka: Automatické opětovné připojení klienta není podporováno produktem IBM MQ classes for Java.

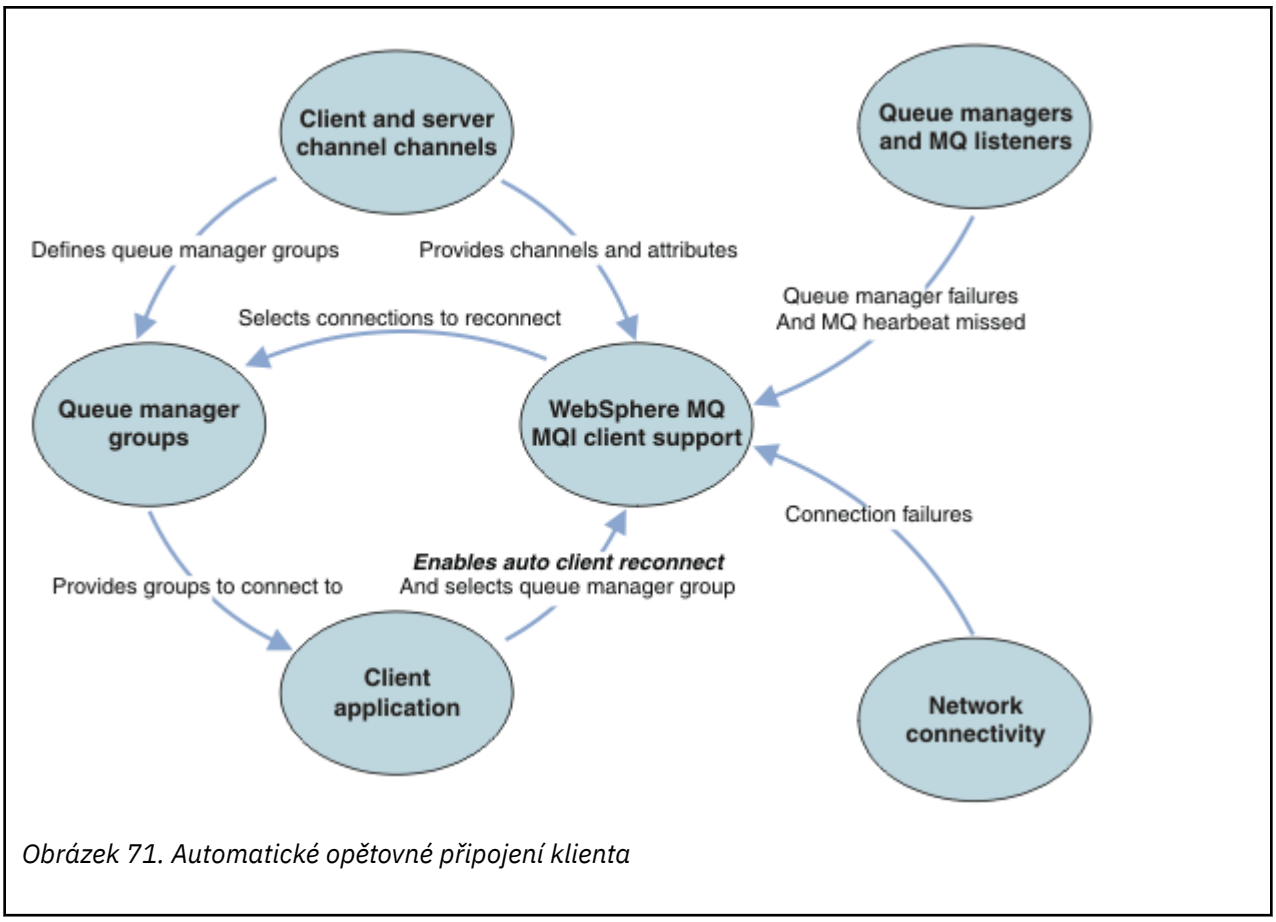
Tabulka 31. Podporovaní klienti			
Rozhraní klienta	**Klient**	**Přístup k programu pro volby opětovného připojení**	**Podpora opětovného připojení**
Rozhraní API systému	C, C + +, COBOL, Nespravovaný Visual Basic, XMS (Nespravované XMS na Windows)	7.0.1	7.0.1
	Kontejner klienta JMS (JSE a Java EE a spravované kontejnery)	7.0.1.3	7.0.1.3
	IBM MQ classes for Java	Nepodporováno	Nepodporováno
	Spravované klienty XMS a spravované klienti .NET : C#, Visual Basic,	7.1	7.1
Jiná rozhraní API	Windows Communication Foundation (Nespravovaný [1])	Nepodporováno	7.0.1
	Windows Communication Foundation (Spravováno [1])	Nepodporováno	Nepodporováno
	Osa 1	Nepodporováno	Nepodporováno
	Osa 2	Nepodporováno	7.0.1.3
	HTTP (web 2.0)	Nepodporováno	7.0.1.3

1. Nastavení spravovaného nebo nespravovaného režimu v konfiguraci vazby WCF.

Automatické opětovné připojení má následující požadavky na konfiguraci:

Tabulka 32. Požadavky na konfiguraci automatického opětovného připojení		
Komponenta	**Požadavek**	**Vliv nesplnění požadavku**
instalace produktu IBM MQ MQI client	Viz téma Tabulka 31 na stránce 420	`MQRC_OPTIONS_ERROR`
Instalace serveru IBM MQ	Úroveň 7.0.1	`MQRC_OPTIONS_ERROR`
Kanál	`SHARECNV > 0`	`MQRC_ENVIRONMENT_ERROR`
prostředí aplikace	Musí být vláknový	`MQRC_ENVIRONMENT_ERROR`
MQI	Jedna z možností: • `MQCONNX` s volbami `MQCNE Volby` nastaveným na hodnotu `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR`. • `Defrecon=YES|QMGR` in `mqclient.ini` • V JMS nastavte vlastnost **`CLIENTRECONNECTOPTIONS`** továrny připojení.	`MQCC_FAILED` je-li připojení přerušeno nebo selže nebo selže správce front.

Produkt Obrázek 71 na stránce 421 zobrazuje hlavní interakce mezi komponentami, které jsou zapojeny do opětovného připojení klienta.



Obrázek 71. Automatické opětovné připojení klienta

Aplikace klienta

Klientská aplikace je IBM MQ MQI client. Podrobnosti o automatickém novém připojení klienta pro klienta JMS naleznete v tématu Použití automatického připojení klienta JMS.

- Ve výchozím nastavení nejsou klienti automaticky znovu připojeni. Povolte automatické opětovné připojení klienta nastavením volby `MQCONNX` `MQCNO` `Option` `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR`.
- Mnoho aplikací je napsáno takovým způsobem, že jsou schopni využít výhod automatického opětovného připojení bez dalšího kódování. Povolte automatické opětovné připojení pro existující programy, bez provedení jakýchkoli změn kódu, nastavením atributu `DefRecon` ve stanze kanálů konfiguračního souboru `mqclient.ini` .
- Použijte jednu z těchto tří voleb:

  1. Upravte program tak, aby logika nebyla ovlivněna opětovným připojením. Například může být nutné volat volání `MQI` v rámci synchronizačního bodu a znovu odeslat zálohované transakce.
  2. Přidejte obslužnou rutinu událostí pro zjištění opětovného připojení a obnovte stav aplikace klienta při opětovném navázání připojení.
  3. Nepovolit automatické opětovné připojení: namísto toho odpojte klienta a zadejte nové volání `MQI` produktu `MQCONN` nebo `MQCONNX` k nalezení jiné instance správce front, která je spuštěna ve stejné skupině správců front.

  Další podrobnosti o těchto třech volbách naleznete v tématu “Obnova aplikace” na stránce 507.
- Opětovné připojení ke správci front se stejným názvem nezaručuje, že jste se znovu připojili ke stejné instanci správce front.

Použijte volbu MQCNO MQCNO_RECONNECT_Q_MGR, chcete-li se znovu připojit k instanci stejného správce front.

- Klient může registrovat obslužnou rutinu událostí tak, aby mohl být informován o stavu opětovného připojení. MQHCONN poslanou v obslužné rutině událostí nelze použít. K dispozici jsou následující kódy příčiny:

  PŘIPOJENÍ MQRC_RECONNECTING
  Připojení se nezdařilo a systém se pokouší znovu navázat spojení. Pokud je provedeno více pokusů o opětovné připojení, obdržíte více událostí produktu MQRC_RECONNECTING .

  MQRC_RECONNECTED
  Provedené opětovné připojení a všechny obslužné rutiny byly úspěšně znovu vytvořeny.

  SELHÁNÍ OPERACE MQRC_RECONNECT_FAILED
  Nové připojení nebylo úspěšné.

  FUNKCE MQRC_RECONNECT_QMID_MISMATCH
  Bylo zadáno připojení s možností opětovného připojení MQCNO_RECONNECT_Q_MGR a připojení se pokusilo znovu připojit k jinému správci front.

  POŽ. Q_MGR_QM_Q_MGR_QM_Q_MGR_
  V klientském programu, který vyžaduje opětovné připojení ke stejnému správci front, byla v klientském programu uvedena volba, například MQMO_MATCH_MSG_TOKEN ve volání MQGET .

- Reconnectable klient se může znovu připojit automaticky pouze po navázání spojení. To znamená, že volání MQCONNX samo o sobě se nepokusí znovu, pokud selže. Pokud například obdržíte návratový kód 2543 - MQRC_STANDBY_Q_MGR z MQCONNX, znovu zadejte volání po krátké prodlevě.

  MQRC_RECONNECT_INCOMPATIBLE
  Tento kód příčiny je vrácen při pokusu aplikace o použití produktu MQPMO_LOGICAL_ORDER (příkazy MQPUT a MQPUT1) nebo MQGMO_LOGICAL_ORDER (s MQGET). jsou-li nastaveny volby opětného připojení. Důvod vrácení kódu příčiny spočívá v tom, že aplikace se v takových případech nikdy znovu nevyužívají.

  MQRC_CALL_INTERRUPTED
  Tento kód příčiny je vrácen při přerušení připojení během provádění volání Commit a opětovného připojení klienta. MQPUT trvalé zprávy mimo synchronizační bod má za následek vrácení kódu příčiny do aplikace.

Správci front vysoké dostupnosti

Správci front s vysokou dostupností mají aktivní instanci a jednu nebo více instancí v pohotovostním režimu pro správce front. Aktivní správce front je synchronizován se správci front v pohotovostním režimu, takže rezervní databáze se může automaticky převzít, pokud selže aktivní instance. Existuje řada různých řešení, která poskytují správce front s vysokou dostupností, viz “Konfigurace vysoké dostupnosti” na stránce 429.

Můžete zjednodušit restartování aplikací produktu IBM MQ MQI client poté, co správce front s vysokou dostupností aktivoval svou instanci v pohotovostním režimu, a to pomocí automatického opětovného připojení klienta.

Rezervní instance správce front s vysokou dostupností je obvykle na jiné síťové adrese pro aktivní instanci. Zahrnout síťové adresy obou instancí v tabulce definic připojení klienta (CCDT). Zadejte buď seznam síťových adres pro parametr **CONNAME** , nebo definujte více řádků pro správce front v tabulce CCDT. Replikované správce datových front a správci front vysoké dostupnosti zařízení IBM MQ podporují plovoucí adresy IP, kde uvedete jednu adresu pro použití s aktivními nebo pohotovostními správci front.

Skupiny správců front

Běžně se produkt IBM MQ MQI clients znovu připojí ke kterémukoli správci front ve skupině správců front. Někdy chcete, aby se produkt IBM MQ MQI client znovu připojil pouze ke stejnému správci front. Může mít afinitu ke správci front.

Můžete vybrat, zda se klientská aplikace vždy připojí a znovu připojí ke správci front se stejným názvem, ke stejnému správci front nebo k některé ze sady správců front, které jsou definovány se stejnou hodnotou QMNAME v tabulce připojení klienta.

- Atribut názvu správce front QMNAMEje v definici kanálu klienta názvem skupiny správců front.
- Pokud v aplikaci klienta nastavíte hodnotu parametru MQCONN nebo MQCONNX QmgrName na název správce front, připojí se klient pouze ke správcům front s tímto názvem. Pokud zadáte předponu názvu správce front s hvězdičkou (*), klient se připojí ke kterémkoli správci front ve skupině správců front se stejnou hodnotou proměnné QMNAME . Úplné vysvětlení naleznete v tématu Skupiny správců front v tabulce CCDT.

Klienta můžete zabránit tak, aby se znovu připojili k jinému správci front. Nastavte volbu MQCNO , MQCNO_RECONNECT_Q_MGR. Pokud se produkt IBM MQ MQI client znovu připojí k jinému správci front, dojde k selhání. Nastavíte-li volbu MQCNO , MQCNO_RECONNECT_Q_MGR, nezahrnujte do stejné skupiny správců front další správce front. Klient vrátí chybu, pokud se správce front, k němuž se znovu připojuje, nejedná o stejného správce front jako ten, k němuž je připojen.

Skupiny sdílení front

z/OS Automatické opětovné připojení klienta ke skupinám sdílení front produktu z/OS používá stejné mechanizmy pro opětovné připojení jako kterékoli jiné prostředí. Klient se znovu připojí ke stejnému výběru správců front, jak je nakonfigurováno pro původní připojení. Například při použití tabulky definic kanálů klienta by měl administrátor zajistit, aby všechny záznamy v tabulce byly interpretovatelné na stejnou skupinu sdílení front produktu z/OS .

Definice kanálů klienta a serveru

Definice kanálů klienta a serveru definují skupiny správců front, ke kterým se může klientská aplikace znovu připojit. Definice řídí výběr a časování opětovného připojení a další faktory, jako např. zabezpečení; viz související témata. Nejrelevantnější atributy kanálu, které se mají zvážit pro opětovné připojení, jsou vypsány ve dvou skupinách:

Atributy připojení klienta
Afinita připojení (AFFINITY) AFFINITY
Příbuznost připojení.

Váha kanálu klienta (CLNTWGHT) CLNTWGHT
Váha připojení klienta.

Název připojení (CONNAME) CONNAME
Informace o připojení.

Interval prezenčního signálu (HBINT) HBINT
Interval prezenčního signálu. Nastavte interval prezenčního signálu na kanálu připojení serveru.

Interval udržení aktivity (KAINT) KAINT
Interval udržení aktivity. Nastavte interval udržení aktivity na kanálu připojení serveru.

z/OS Všimněte si, že KAINT se vztahuje pouze na z/OS .

Název správce front (QMNAME) QMNAME
Název správce front.

Atributy připojení serveru
Interval prezenčního signálu (HBINT) HBINT
Interval prezenčního signálu. Nastavte interval prezenčního signálu na kanálu připojení klienta.

Interval udržení aktivity (KAINT) KAINT
Interval udržení aktivity. Nastavte interval udržení aktivity na kanálu připojení klienta.

z/OS Všimněte si, že KAINT se vztahuje pouze na z/OS .

KAINT je prezenční signál síťové vrstvy a HBINT je prezenční signál produktu IBM MQ mezi klientem a správcem front. Nastavení těchto synchronizačních signálů po kratší dobu slouží ke dvěma účelům:

1. Simulací aktivity na připojení je méně pravděpodobné, že by síť síťového vrstvy, která je zodpovědná za uzavření neaktivních připojení, vypnula vaše připojení.
2. Je-li připojení ukončeno, je zkráceno zpoždění před tím, než dojde k přerušení nefunkčních připojení.

Výchozí interval udržení aktivity TCP/IP je dvě hodiny. Zvažte nastavení atributů KAINT a HBINT na kratší dobu. Nepředpokládejte, že normální chování sítě vyhovuje potřebám automatického opětovného připojení. Například některé brány firewall mohou vypnout neaktivní připojení TCP/IP po uplynutí pouhých 10 minut.

Síťová konektivita

Pouze selhání sítě, která jsou předávána síti IBM MQ MQI client , jsou obsluhována schopností automatického opětovného připojení klienta.

- Opětovné připojení provedená automaticky přenosem je neviditelná pro IBM MQ.
- Nastavení HBINT pomáhá vypořádat se se selháními sítě, která jsou neviditelná pro produkt IBM MQ.

Správci front a moduly listener produktu IBM MQ

Přepojení klienta se spouští selháním serveru, selháním správce front, selháním síťového připojení a přepojením administrátora na jinou instanci správce front.

- Pokud používáte správce front s více instancemi, vyskytne se při přepnutí řízení z aktivní instance správce front na instanci v pohotovostním režimu další příčina opakovaného připojení klienta.
- Ukončení správce front s použitím výchozího příkazu **endmqm** nespouští automatické opětovné připojení klienta. Přidejte volbu `-r` do příkazu **endmqm** , chcete-li požádat o automatické opětovné připojení klienta, nebo volbu `-s` pro přenos na instanci správce front v pohotovostním režimu po jeho ukončení.

Podpora automatického opětovného připojení produktu IBM MQ MQI client

Pokud použijete podporu automatického připojení klienta v produktu IBM MQ MQI client, klientská aplikace se automaticky znovu připojí a pokračuje ve zpracování bez zadání volání MQI MQCONN nebo MQCONNX k opětovnému připojení ke správci front.

- Automatické opětovné připojení klienta se spustí jedním z následujících výskytů:
  - Selhání správce front
  - Ukončení správce front s určením volby `-r`, opětovného připojení, volby v příkazu **endmqm**
- Volby produktu MQCONNX MQCNO řídí, zda jste povolili automatické opětovné připojení klienta. Volby jsou popsány v části Volby opětovného připojení.
- Automatické opětovné připojení klienta vydává volání MQI jménem vaší aplikace k obnovení manipulátoru připojení a obslužných rutin k dalším otevřeným objektům, takže váš program může pokračovat v běžném zpracování poté, co zpracoval jakékoli chyby MQI, které měly za následek nefunkční připojení. Viz “Zotavení automaticky znovu připojeného klienta” na stránce 509.
- Pokud jste pro připojení napsali uživatelský program kanálu, tato uživatelská procedura obdrží tato další volání MQI.
- Můžete registrovat obslužnou rutinu událostí opětovného připojení, která se spustí při zahájení opětovného připojení a kdy skončí.

Ačkoli zamýšlená doba opětného připojení není delší než minuta, opětovné připojení může trvat déle, protože správce front může mít mnoho prostředků, které lze spravovat. Během této doby může klientská aplikace zadržovat zámky, které nenáleží k prostředkům produktu IBM MQ . Existuje hodnota časového limitu, kterou můžete nakonfigurovat k omezení doby, po kterou klient čeká na opětovné připojení. Hodnota (v sekundách) je nastavena v souboru `mqclient.ini` .

```
Channels:
MQReconnectTimeout = 1800
```

Po vypršení časového limitu nejsou provedeny žádné pokusy o opětovné připojení. Když systém zjistí, že vypršel časový limit, vrátí chybu MQRC_RECONKTI_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 provozovat správce front produktu IBM MQ v konfiguraci vysoké dostupnosti (HA), můžete nastavit správce front tak, aby pracoval buď se správcem funkce vysoké dostupnosti, například PowerHA for AIX (dříve HACMP). nebo Microsoft Cluster Service (MSCS) nebo se správcem front IBM MQ s více instancemi. V 9.1.0 Na systémech Linux můžete také implementovat replikované správce datových front (RQMs), které využívají skupinu založenou na kvótě k zajištění vysoké dostupnosti.

MQ Appliance Další možností řešení vysoké dostupnosti nebo zotavení z havárie je implementovat pár zařízení produktu IBM MQ . Viz High Availability a Disaster Recovery v dokumentaci produktu IBM MQ Appliance .

Je třeba, abyste si byli vědomi následujících definic konfigurace:

Klastry správců front
Skupiny dvou nebo více správců front na jednom nebo více počítačích, poskytují automatické propojení a umožňují sdílení front mezi nimi pro vyrovnávání zátěže a redundanci. Počínaje produktem IBM WebSphere MQ 7.1 operace zotavení z chyb klastru spouští operace, které způsobily problémy, dokud nejsou vyřešeny problémy.

Klastry HA
Klastry s vysokou dostupností jsou skupiny dvou nebo více počítačů a prostředků, jako jsou disky a sítě, propojené a nakonfigurované takovým způsobem, že pokud dojde k selhání, správce funkce vysoké dostupnosti, jako například HACMP (UNIX) nebo MSCS (Windows) provádí *přepnutí při selhání*. Překonání selhání přenese stavová data aplikací ze selhávajícího počítače na jiný počítač v klastru a znovu iniciuje jejich činnost. Poskytuje vysokou dostupnost služeb spuštěných v klastru s vysokou dostupností. Vztah mezi klastry produktu IBM MQ a klastry HA je popsán v tématu “Vztah klastrů s vysokou dostupností do klastrů správců front” na stránce 430.

Správci front s více instancemi
Instance stejného správce front konfigurované ve dvou nebo více počítačích. Spouští se více instancí, jedna instance se stane aktivní instancí a ostatní instance se stanou standbys. Dojde-li k selhání aktivní instance, automaticky převezme rezervní instanci běžící na jiném počítači. Pomocí správců front s více instancemi můžete nakonfigurovat své vlastní vysoce dostupné systémy zasílání zpráv založené na produktu IBM MQbez nutnosti použití klastrové technologie, jako je HACMP nebo MSCS. Klastry s vysokou dostupností a správci front s více instancemi jsou alternativní způsoby, jak správci front zpřístupnit vysokou dostupnost. Nekombinujte je umístěním správce front s více instancemi do klastru s vysokou dostupností.

V 9.1.0 **Replikované správce front dat s vysokou dostupností (HA RQMs)**
Instance stejného správce front, které jsou konfigurovány na každém uzlu ve skupině tří serverů Linux . Jedna ze tří instancí je aktivní instance. Data z aktivního správce front jsou synchronně

replikována do ostatních dvou instancí, takže jedna z těchto instancí může v případě nějakého selhání převzít. Seskupení serverů je řízeno Pacemakera replikace podle DRBD.

V 9.1.0 **Replikované správci datových front pro zotavení z havárie (DR RQMs)**
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 se replikují mezi primární instancí a sekundární instancí, a pokud je primární uzel z nějakého důvodu ztracen, sekundární instanci může být provedena do primární instance a spuštěna. Oba uzly musí být servery Linux . Replikace je řízena DRBD.

Rozdíly mezi správci front s více instancemi a klastry HA

Správci front s více instancemi a klastry s vysokou dostupností jsou alternativní způsoby, jak dosáhnout vysoké dostupnosti pro správce front. Zde jsou některé body, které zdůrazňují rozdíly mezi oběma přístupy.

Správci front s více instancemi zahrnují následující funkce:

- Základní podpora překonání selhání integrovaná do produktu IBM MQ
- Rychlejší překonání selhání než klastr HA
- Jednoduchá konfigurace a operace
- Integrace s produktem IBM MQ Explorer

Omezení správců front s více instancemi zahrnují:

- jsou k dispozici vysoce výkonné síťové úložiště, které je k dispozici
- Složitější konfigurace sítě, protože správce front změní IP adresu, když selže

Klastry HA zahrnují následující funkce:

- Schopnost koordinovat více prostředků, jako je například aplikační server nebo databáze.
- Flexibilnější možnosti konfigurace včetně klastrů zahrnujících více než dva uzly.
- Může překonávání selhání bez zásahu operátora bez obsluhy.
- Převzetí adresy IP správce front jako součásti překonání selhání

Omezení klastrů HA zahrnuje:

- Je třeba zakoupit další nákup produktů a dovednosti.
- Disky, které lze přepínat mezi uzly klastru, jsou povinné.
- Konfigurace klastrů HA je relativně složitá
- Překonání selhání je historicky poměrně pomalé, ale nedávné produkty klastru HA se zlepšují.
- Nepotřebné překonání selhání se mohou vyskytnout, pokud existují nedostatky ve skriptech, které se používají k monitorování prostředků, jako jsou správci front.

Vztah klastrů s vysokou dostupností do klastrů správců front

Klastry správců front poskytují vyrovnávání zátěže zpráv mezi dostupnými instancemi front klastru správce front. Tato nabídka nabízí vyšší dostupnost než jeden správce front, protože po selhání správce front mohou aplikace systému zpráv i nadále odesílat zprávy a přistupovat k přeživovaným instancím fronty klastru správce front. Ačkoli však klastry správců front automaticky přesměrují nové zprávy do dostupných správců front v klastru, zprávy aktuálně zařazené do nedostupného správce front nebudou k dispozici, dokud nebude správce front restartován. Z tohoto důvodu samy klastry správců front neposkytují vysokou dostupnost všech dat zpráv nebo poskytují automatickou detekci selhání správce front a automatické spouštění restartování správce front nebo překonání selhání. Klastry vysoké dostupnosti (HA) poskytují tyto funkce. Tyto dva typy klastrů lze použít společně s dobrým účinkem. Úvod do klastrů správců front naleznete v tématu Navrhování klastrů.

Související úlohy

V 9.1.4 MQ Adv. Linux CD Vysoká dostupnost pro IBM MQ Advanced certified container

Linux UNIX Klastry HA na systému UNIX and Linux

Můžete použít produkt IBM MQ s klastrem s vysokou dostupností (HA) na platformách UNIX and Linux , například PowerHA pro AIX (dříve HACMP), Veritas Cluster Server, HP Serviceguard nebo klastr Red Hat Enterprise Linux s Red Hat Cluster Suite.

Před IBM WebSphere MQ 7.0.1byl poskytnut produkt SupportPac MC91 , který vám pomůže při konfiguraci klastrů HA. Produkt IBM WebSphere MQ 7.0.1 poskytl vyšší stupeň kontroly než předchozí verze, kdy správci front ukládají svá data. Díky tomu je snazší konfigurovat správce front v klastru s vysokou dostupností. Většina skriptů poskytnutých s produktem SupportPac MC91 již není vyžadována a balík SupportPac je stažen.

Tento oddíl představuje “Konfigurace klastru vysoké dostupnosti” na stránce 431, vztah klastrů s vysokou dostupností do klastrů správců front, “IBM MQ klienti” na stránce 432a “IBM MQ pracující v klastru s vysokou dostupností” na stránce 432, a vás provede jednotlivými kroky a poskytuje ukázkové skripty, které můžete upravit, chcete-li nakonfigurovat správce front s klastrem s vysokou dostupností.

V dokumentaci ke klastru s vysokou dostupností se podívejte do dokumentace ke konfiguraci klastru popsaného v této části týkající se vašeho prostředí pro spolupráci s vysokou dostupností.

Konfigurace klastru vysoké dostupnosti

V tomto oddílu je výraz *uzel* použit jako odkaz na entitu, na které běží operační systém a software HA; "počítač", "systém" nebo "počítač" nebo "logická oblast" nebo "blade" mohou být považovány za synonyma v tomto použití. Produkt IBM MQ můžete použít k nastavení buď záložních nebo přejímacích konfigurací, včetně vzájemného převzetí, kde všechny uzly klastru pracují se IBM MQ pracovní zátěží.

Konfigurace *rezervní databáze* je nejzákladnější konfigurací klastru vysoké dostupnosti, v níž jeden uzel provádí práci, zatímco druhý uzel funguje pouze jako rezervní. Záložní uzel neprovedl práci a je označen jako nečinný; tato konfigurace se někdy nazývá *studený pohotovostní režim*. Taková konfigurace vyžaduje vysoký stupeň redundance hardwaru. Chcete-li šetřit na hardwaru, je možné rozšířit tuto konfiguraci tak, aby měla více pracovních uzlů s jedním rezervním uzlem. Poukazuje na to, že záložní uzel může převzít práci všech ostatních pracovních uzlů. Tato konfigurace je stále označována jako záložní konfigurace a někdy také jako konfigurace "N+1".

Převzetí konfigurace je pokročilejší konfigurací, v níž všechny uzly provádějí určitou práci a v případě selhání uzlu je možné převzít práci v rámci kritického zpracování.

Konfigurace *jednostranného převzetí* je jedna z nich, v níž záložní uzel provádí některé další, nekritické a nepřenosné práce. Tato konfigurace je podobná konfiguraci rezervní databáze, ale s (nekritickou) prací prováděnou záložním uzlem.

Konfigurace *mutual takeover* je ta, ve které všechny uzly provádějí vysoce dostupné (pohyblivé) práce. Tento typ konfigurace klastru s vysokou dostupností je někdy také označován jako "Aktivní/Aktivní", což znamená, že všechny uzly aktivně zpracovávají kritickou pracovní zátěž.

S rozšířenou rezervní konfigurací nebo některou z konfigurací převzetí je důležité zvážit maximální zatížení, které může být umístěno na uzlu, který může převzít práci jiných uzlů. Takový uzel musí mít dostatečnou kapacitu, aby udržel přijatelnou úroveň výkonu.

Vztah klastrů s vysokou dostupností do klastrů správců front

Klastry správců front snižují administraci a poskytují vyrovnávání zátěže zpráv v rámci instancí front klastru správce front. Nabízejí také vyšší dostupnost než jeden správce front, protože po selhání správce front mohou aplikace systému zpráv i nadále přistupovat k přežívím ve frontě klastru správce front. Samotné klastry správců front však neposkytují automatickou detekci selhání správce front a automatické

spouštění restartování správce front nebo překonání selhání. Klastry vysoké dostupnosti poskytují tyto funkce. Tyto dva typy klastrů lze použít společně s dobrým účinkem.

IBM MQ klienti

Klienti IBM MQ , kteří komunikují se správcem front, který může být předmětem restartování nebo převzetí, musí být napsány tak, aby tolerovali přerušené připojení a opakovaně se musí pokusit o připojení znovu. Produkt IBM WebSphere MQ 7 zavádí funkce v rámci zpracování tabulky CCDT (Client Channel Definition Table), které pomáhají při dostupnosti připojení a vyrovnávání pracovní zátěže. Tyto funkce však nejsou přímo relevantní při práci se systémem překonání selhání.

Transakční funkčnost umožňuje produktu IBM MQ MQI client podílet se na dvoudfázových transakcích, pokud je klient připojen ke stejnému správci front. Transakční funkčnost nemůže použít techniky, jako např. prostředek pro rozložení zátěže IP, vybírat ze seznamu správců front. Pokud používáte produkt HA, udržuje správce front svou identitu (název a adresa), na kterémkoliv uzlu běží, takže transakční funkčnost může být použita se správci front, kteří jsou pod kontrolou funkce HA.

IBM MQ pracující v klastru s vysokou dostupností

Všechny klastry HA mají koncept jednotky překonání selhání. Jedná se o sadu definic, které obsahují všechny prostředky, které tvoří vysoce dostupnou službu. Jednotka překonání selhání zahrnuje samotnou službu a všechny ostatní prostředky, na kterých závisí.

Řešení vysoké dostupnosti používají odlišné podmínky pro jednotku překonání selhání:

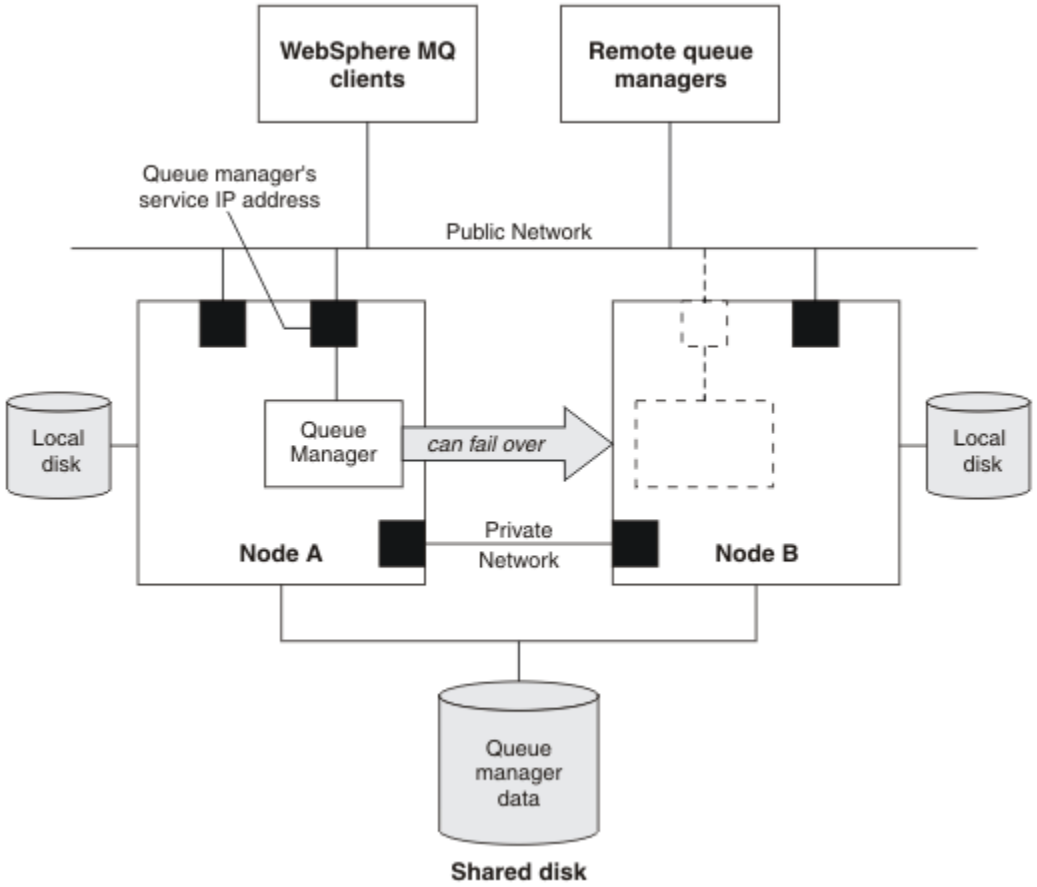
- V systémech PowerHA for AIX se jednotka překonání selhání nazývá *skupina prostředků*.
- Na serveru Veritas Cluster Server je znám jako *skupina služeb*.
- Na Serviceguard se nazývá *balík*.

Toto téma používá termín *skupina prostředků* k označení jednotky překonání selhání.

Nejmenší jednotka překonání selhání pro produkt IBM MQ je správce front. Obvykle skupina prostředků obsahující správce front také obsahuje sdílené disky ve skupině svazků nebo ve skupině disků, které jsou vyhrazeny výhradně pro použití skupinou prostředků, a dále adresa IP, která se používá pro připojení ke správci front. Je také možné zahrnout jiné prostředky produktu IBM MQ , jako např. modul listener nebo monitor spouštěčů ve stejné skupině prostředků, buď jako samostatné prostředky, nebo pod řízením správce front jako takového.

Správce front, který má být použit v klastru s vysokou dostupností, musí mít svá data a protokoly na discích, které jsou sdíleny mezi uzly v klastru. Klastr HA zajišťuje, že v daném okamžiku může zapisovat na disky pouze jeden uzel v klastru. Klastr s vysokou dostupností může ke sledování stavu správce front použít skript monitoru.

Je možné použít jeden sdílený disk jak pro data, tak pro protokoly, které souvisejí se správcem front. Je však běžnou praxí používat samostatné sdílené systémy souborů tak, aby mohly být nezávisle dimenzovány a vyladěny.



Obrázek 72. Klastr vysoké dostupnosti

Obrázek 1 ilustruje klastr s vysokou dostupností se dvěma uzly. Klastr vysoké dostupnosti spravuje dostupnost správce front, který byl definován ve skupině prostředků. Jedná se o aktivní/pasivní nebo studenou záložní konfiguraci, protože pouze jeden uzel, uzel A, momentálně spouští správce front. Správce front byl vytvořen se svými daty a soubory protokolu na sdíleném disku. Správce front má adresu IP služby, která je spravována také klastrem HA. Správce front závisí na sdíleném disku a na jeho adrese IP služby. Selže-li klastr vysoké dostupnosti správce front z uzlu A do uzlu B, přesune nejprve na uzel B závislé prostředky správce front a poté spustí správce front.

Pokud klastr s vysokou dostupností obsahuje více než jednoho správce front, může konfigurace klastru s vysokou dostupností vést ke spuštění dvou nebo více správců front spuštěných ve stejném uzlu po překonání selhání. Každému správci front v klastru s vysokou dostupností musí být přiřazeno vlastní číslo portu, které používá v libovolném uzlu klastru, který má být aktivní v libovolném konkrétním čase.

Obecně je klastr vysoké dostupnosti spuštěn jako uživatel root. Produkt IBM MQ se spouští jako uživatel mqm. Administrace produktu IBM MQ je poskytována členům skupiny mqm. Ujistěte se, že uživatel mqm a skupina existují na všech uzlech klastru vysoké dostupnosti. ID uživatele a ID skupiny musí být konzistentní v rámci klastru. Administrace produktu IBM MQ uživatelem root není povolena; skripty, které spouštějí, zastavují nebo monitorují skripty, se musí přepnout na uživatele mqm.

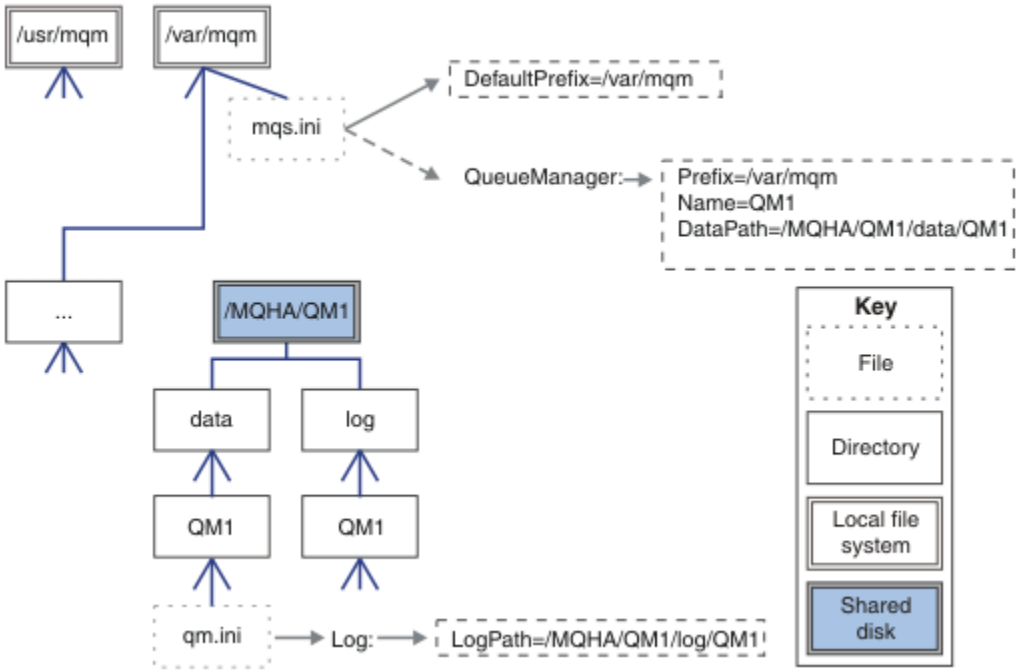
Poznámka: Produkt IBM MQ musí být instalován správně na všech uzlech; nelze sdílet spustitelné soubory produktu.

Linux UNIX *Konfigurace sdílených disků v systému UNIX and Linux*

Správce front IBM MQ v klastru s vysokou dostupností vyžaduje, aby datové soubory a soubory protokolu byly ve společném pojmenovaném vzdáleném systému souborů na sdíleném disku.

Informace o této úloze

Obrázek 1 znázorňuje možné rozvržení pro správce front v klastru vysoké dostupnosti. Data a adresáře protokolů správce front jsou umístěny na sdíleném disku, který je připojen v adresáři /MQHA/QM1. Tento disk je přepnut mezi uzly klastru s vysokou dostupností, pokud dojde k překonání selhání, aby byla data dostupná všude, kde je správce front restartován. Soubor `mqs.ini` obsahuje sekci pro správce front QM1 . Sekce Protokol v souboru `qm.ini` má hodnotu pro LogPath.



Obrázek 73. Sdíleno s názvy adresářů `data` a `log`

Postup

1. Rozhodněte se pro názvy bodů připojení pro systémy souborů správce front.

   Například, `/MQHA/qmgrname/data` pro datové soubory správce front a `/MQHA/qmgrname/log` pro své soubory protokolu.
2. Vytvořte skupinu disků (nebo skupinu disků), která bude obsahovat data a soubory protokolu správce front.

   Tato skupina disků je spravována klastrem vysoké dostupnosti (HA) ve stejné skupině prostředků jako správce front.
3. Vytvořte systémy souborů pro data správce front a soubory protokolu ve skupině svazků.
4. Pro každý uzel dále vytvořte body připojení pro systémy souborů a ujistěte se, že je možné připojit systémy souborů.

   Uživatel mqm musí vlastnit body připojení.

Linux UNIX *Vytvoření správce front klastru vysoké dostupnosti v systému UNIX and Linux*

Prvním krokem směrem k použití správce front v klastru s vysokou dostupností je vytvoření správce front v jednom z těchto uzlů.

Informace o této úloze

Chcete-li vytvořit správce front pro použití v klastru s vysokou dostupností, musíte nejprve vybrat jeden z uzlů v klastru, v němž se má vytvořit správce front, a poté na tomto uzlu provést následující kroky.

Postup

1. Připojte systémy souborů správce front v daném uzlu.
2. Vytvořte správce front pomocí příkazu **crtmqm** .
   Příklad:

   ```
   crtmqm -md /MQHA/qmgrname/data -ld /MQHA/qmgrname/log qmgrname
   ```
3. Spusťte správce front ručně pomocí příkazu **strmqm** .
4. Dokončete veškeré počáteční konfigurace správce front, jako je například vytváření front a kanálů, a nastavení správce front tak, aby se modul listener spustil automaticky při spuštění správce front.
5. Zastavte správce front pomocí příkazu **endmqm** .
6. Chcete-li zobrazit příkaz **addmqinf** , použijte příkaz **dspmqinf** :

   ```
   dspmqinf -o command qmgrname
   ```

   kde `qmgrname` je název správce front.

   Další informace o použití příkazu **addmqinf** naleznete v tématu “Přidání konfigurace správce front do jiných uzlů klastru vysoké dostupnosti v systému UNIX and Linux” na stránce 435.

   Příkaz **addmqinf** se zobrazuje podobným způsobem jako v následujícím příkladu:

   ```
   addmqinf -sQueueManager -vName=qmgrname -vDirectory=qmgrname \
   -vPrefix=/var/mqm -vDataPath=/MQHA/qmgrname/data/qmgrname
   ```
7. Pečlivě si všimněte zobrazeného příkazu.
8. Odpojte systémy souborů správce front.

Jak pokračovat dále

Nyní jste připraveni dokončit kroky popsané v tématu “Přidání konfigurace správce front do jiných uzlů klastru vysoké dostupnosti v systému UNIX and Linux” na stránce 435.

Linux UNIX *Přidání konfigurace správce front do jiných uzlů klastru vysoké dostupnosti v systému UNIX and Linux*

Informace o konfiguraci správce front je třeba přidat do ostatních uzlů v klastru s vysokou dostupností.

Než začnete

Před provedením této úlohy musíte provést kroky uvedené v tématu “Vytvoření správce front klastru vysoké dostupnosti v systému UNIX and Linux” na stránce 434. Po vytvoření správce front je třeba přidat informace o konfiguraci správce front do všech ostatních uzlů v klastru s vysokou dostupností tak, že na každém z ostatních uzlů provedete následující kroky.

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 vysoké dostupnosti v systému UNIX and Linux” na stránce 434.

Postup

1. Připojte systémy souborů správce front.
2. Přidejte informace o konfiguraci správce front do uzlu.
   Existují dva způsoby, jak přidat informace o konfiguraci:
   - Úpravou `/var/mqm/mqs.ini` přímo.

- Vydáním příkazu **addmqinf** , který byl zobrazen příkazem **dspmqinf** v kroku 6 v příručce “Vytvoření správce front klastru vysoké dostupnosti v systému UNIX and Linux” na stránce 434.

3. Spuštěním a zastavením správce front ověřte konfiguraci.

   Příkazy použité ke spuštění a zastavení správce front musí být zadány ze stejné instalace IBM MQ jako příkaz **addmqinf** . Chcete-li správce front spustit a zastavit z jiné instalace než z té, která je aktuálně asociována se správcem front, je třeba nejprve nastavit instalaci přidruženou ke správci front pomocí příkazu **setmqm** . Další informace viz setmqm.
4. Odpojte systémy souborů správce front.

Linux UNIX *Ukázkové skripty shellu pro spuštění správce front klastru vysoké dostupnosti v systému UNIX and Linux*

Správce front je reprezentován v klastru vysoké dostupnosti jako prostředek. Klastr s vysokou dostupností musí být schopen spustit a zastavit správce front. Ve většině případů můžete ke spuštění správce front použít skript shellu. Tyto skripty musíte zpřístupnit ve stejném umístění na všech uzlech v klastru, a to buď pomocí síťového systému souborů, nebo jejich zkopírováním na každý z lokálních disků.

Poznámka: Před restartováním správce front, který selhal, je třeba odpojit vaše aplikace od této instance správce front. Pokud tomu tak není, nemusí se správce front restartovat správně.

Zde jsou uvedeny příklady vhodných skriptů shellu. Tyto vlastnosti můžete upravit podle svých potřeb a použít je ke spuštění správce front pod kontrolou klastru s vysokou dostupností.

Následující skript shellu je příkladem, jak přepnout z uživatele klastru s vysokou dostupností na uživatele mqm, aby mohl být správce front úspěšně spuštěn:

```
#!/bin/ksh

# A simple wrapper script to switch to the mqm user.

su mqm -c name_of_your_script $*
```

Následující skript shellu je příkladem toho, jak spustit správce front bez jakýchkoli předpokladů týkajících se aktuálního stavu správce front. Všimněte si, že používá extrémně náhlý způsob ukončení všech procesů, které patří ke správci front:

```
#!/bin/ksh
#
# This script robustly starts the queue manager.
#
# The script must be run by the mqm user.

# The only argument is the queue manager name. Save it as QM variable
QM=$1

if [ -z "$QM" ]
then
  echo "ERROR! No queue manager name supplied"
  exit 1
fi

# End any queue manager processes which might be running.

srchstr="( |-m)$QM *.*$"
for process in amqzmuc0 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
               amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
               amqzfuma amqzmuf0 amqzmur0 amqzmgr0
 do
  ps -ef | tr "\t" " " | grep $process | grep -v grep | \
    egrep "$srchstr" | awk '{print $2}'| \
       xargs kill -9 > /dev/null 2>&1
done

# It is now safe to start the queue manager.
# The strmqm command does not use the -x flag.
strmqm ${QM}
```

Tento skript můžete upravit tak, aby spouštěl jiné související programy.

Linux UNIX *Příklad skriptu shell pro zastavení správce front klastru vysoké dostupnosti v systému UNIX and Linux*

Ve většině případů můžete ke zastavení správce front použít skript shellu. Zde jsou uvedeny příklady vhodných skriptů shellu. Tyto vlastnosti můžete upravit podle svých potřeb a použít je k zastavení správce front pod kontrolou klastru s vysokou dostupností.

Následující skript je příkladem toho, jak okamžitě zastavit správce front, aniž by byly předpoklady o aktuálním stavu správce front uvedeny. Skript musí být spuštěn uživatelem mqm. Proto může být nezbytné zabalit tento skript do skriptu shellu a přepnout uživatele z uživatele klastru s vysokou dostupností do skupiny mqm. (Příklad skriptu shellu je poskytnut v "Ukázkové skripty shellu pro spuštění správce front klastru vysoké dostupnosti v systému UNIX and Linux" na stránce 436.)

```
#!/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 tom, které procesy jsou spuštěny pro specifického správce front, nemusí být seznam procesů správce front zahrnutých do tohoto skriptu buď úplný seznam, nebo může obsahovat více procesů než procesy, které jsou spuštěny pro daného správce front:

```
for process in amqzmuc0 amqzxma0 amqfcxba amqfqpub amqpcsea amqzlaa0 \
               amqzlsa0 runmqchi runmqlsr amqcrsta amqrrmfa amqrmppa \
               amqzfuma amqzmuf0 amqzmur0 amqzmgr0
```

Proces může být zahrnut do nebo vyloučen z tohoto seznamu na základě toho, která funkce je konfigurována a jaké procesy jsou spuštěny pro specifického správce front. Úplný seznam procesů a informace o zastavení procesů ve specifickém pořadí naleznete v tématu Ruční zastavení správce front v systému UNIX a Linux.

Linux UNIX *Monitorování správce front klastru vysoké dostupnosti v systému UNIX and Linux*

Je obvyklé poskytovat způsob, jak klastr vysoké dostupnosti (HA) pravidelně monitorovat stav správce front. Ve většině případů můžete použít skript shellu pro tento případ. Zde jsou uvedeny příklady vhodných skriptů shellu. Tyto skripty můžete upravit podle svých potřeb a použít je k provádění dalších kontrol monitorování specifických pro vaše prostředí.

V produktu IBM WebSphere MQ 7.1je možné mít více instalací IBM MQ koexistujících na systému. Další informace o více instalacích najdete v tématu Více instalací. Hodláte-li používat skript monitorování přes více instalací, včetně instalací v produktu IBM WebSphere MQ 7.1nebo vyšší, budete možná muset provést některé další kroky. Pokud máte primární instalaci, nebo používáte skript s verzemi staršími než IBM WebSphere MQ 7.1, nemusíte pro použití skriptu zadávat *MQ_INSTALLATION_PATH* . Jinak následující kroky zajišťují, že je *MQ_INSTALLATION_PATH* správně identifikován:

1. Chcete-li identifikovat správné *MQ_INSTALLATION_PATH* pro správce front, použijte příkaz **crtmqenv** z instalace produktu IBM WebSphere MQ 7.1 :

   ```
   crtmqenv -m qmname
   ```

   Tento příkaz vrací správnou hodnotu *MQ_INSTALLATION_PATH* pro správce front určeného parametrem *qmname*.

2. Spusťte skript monitorování s příslušnými parametry *qmname* a *MQ_INSTALLATION_PATH* .

Poznámka: PowerHA for AIX neposkytuje způsob, jak dodat parametr programu monitorování pro správce front. Musíte vytvořit samostatný monitorovací program pro každého správce front, který bude zapouzdřit název správce front. Zde je příklad skriptu použitého v produktu AIX k zapouzdření názvu správce front:

```
#!/bin/ksh
su mqm -c name_of_monitoring_script qmname  MQ_INSTALLATION_PATH
```

kde *MQ_INSTALLATION_PATH* je nepovinný parametr, který určuje cestu k instalaci produktu IBM MQ , ke které je přidružen správce front *název_správce_front* .

Následující skript není robustní na možnost, že produkt **runmqsc** uvázne. Zpravidla jsou klastry vysoké dostupnosti považovány za selhání a jsou pro tuto možnost samy robustní.

Skript však toleruje, že se správce front nachází ve spouštěním stavu. Je to proto, že je běžné, že klastr HA spouští monitorování správce front ihned poté, co jej začal. Některé klastry vysoké dostupnosti rozlišují mezi počáteční fází a spuštěnou fází pro prostředky, ale je třeba nakonfigurovat dobu trvání počáteční fáze. Vzhledem k tomu, že doba potřebná ke spuštění správce front závisí na množství práce, které má provést, je obtížné vybrat maximální dobu, kterou spouští správce front. Vyberete-li příliš nízkou hodnotu, klastr vysoké dostupnosti nesprávně předpokládá, že správce front selhal, když se nespustil. To může mít za následek nekonečnou posloupnost failovers.

Tento skript musí být spuštěn uživatelem mqm; může být proto nezbytné zabalit tento skript do skriptu shellu a přepnout uživatele z uživatele klastru s vysokou dostupností do systému mqm (příklad skriptu shellu je uveden v produktu “Ukázkové skripty shellu pro spuštění správce front klastru vysoké dostupnosti v systému UNIX and Linux” na stránce 436):

```
#!/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 UNIX *Vložení správce front pod ovládací prvek klastru HA v systému UNIX and Linux*

Správce front je třeba konfigurovat pod kontrolou klastru s vysokou dostupností a s použitím adresy IP správce front a sdílených disků.

Informace o této úloze

Chcete-li správce front uložit pod kontrolu klastru s vysokou dostupností, 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, nikoli adresa IP počítače.
2. Ověřte, že klastr HA správně přepíná prostředky mezi uzly klastru a je připraven k řízení správce front.

Linux UNIX *Odstranění správce front klastru vysoké dostupnosti v systému UNIX and Linux*

Je možné, že budete chtít odebrat správce front z uzlu, který již není potřebný ke spuštění správce front.

Informace o této úloze

Chcete-li odebrat správce front z uzlu v klastru s vysokou dostupností, musíte odebrat jeho informace o konfiguraci.

Postup

1. Odeberte uzel z klastru s vysokou dostupností tak, aby se klastr s vysokou dostupností již nepokusil o aktivaci správce front v tomto uzlu.
2. Chcete-li odebrat informace o konfiguraci správce front, použijte následující příkaz **rmvmqinf** :

   `rmvmqinf` *qmgrname*
3. Volitelné: Chcete-li správce front zcela odstranit, použijte příkaz **dltmqm** .

   Důležité: Pamatujte na to, že odstraněním správce front pomocí příkazu **dltmqm** dojde k úplnému odstranění dat a souborů protokolu správce front.

   Pokud jste správce front odstranili, můžete pomocí příkazu **rmvmqinf** odebrat zbývající informace o konfiguraci z ostatních uzlů.

Windows Podpora produktu Microsoft Cluster Service (MSCS)

Zavedení a nastavení serveru MSCS pro podporu překonání selhání virtuálních serverů.

Tyto informace platí pouze pro IBM MQ for Windows .

Služba Microsoft Cluster Service (MSCS) vám umožňuje připojit servery do *klastru*, což poskytuje vyšší dostupnost dat a aplikací a usnadňuje správu systému. MSCS může automaticky zjišťovat a zotavovat se ze selhání serveru nebo aplikací.

MSCS podporuje *překonání selhání virtuálních serverů*, které odpovídají aplikacím, webovým stránkám, tiskovým frontám nebo sdílení souborů (včetně například jejich diskových spindel, souborů a adres IP).

Překonání selhání je proces, při kterém MSCS zjistí selhání v aplikaci na jednom počítači v klastru a ukončí přerušenou aplikaci řádným způsobem, přenese data o stavu do druhého počítače a znovu iniciuje aplikaci.

Tato sekce představuje klastry klastrů MSCS a popisuje nastavení podpory MSCS v následujících sekcích:

- “Představení klastrů MSCS” na stránce 441
- “Nastavení produktu IBM MQ pro klastrování MSCS” na stránce 442

Poté se dozvíte, jak nakonfigurovat produkt IBM MQ pro klastrování MSCS, v následujících sekcích:

- “Vytvoření správce front pro použití se službou MSCS” na stránce 444
- “Přesun správce front do úložiště MSCS” na stránce 445
- “Vložení správce front do ovládacího prvku MSCS” na stránce 446
- “Odebrání správce front z ovládacího prvku MSCS” na stránce 452

A poté poskytne některé užitečné pokyny k použití prostředí MSCS s produktem IBM MQa obsahuje podrobnosti o obslužných programech podpory prostředí MSCS produktu IBM MQ v následujících sekcích:

- “Rady a tipy pro použití MSCS” na stránce 453
- “Podpora obslužných programů MSCS” na stránce 456

Windows *Představení klastrů MSCS*

Klastry MSCS jsou skupiny dvou nebo více počítačů, které jsou vzájemně propojeny a nakonfigurovány tak, že pokud jeden z nich selže, MSCS provede *přepnutí při selhání*, převede stavová data aplikací ze selhávajícího počítače na jiný počítač v klastru a znovu iniciuje jejich činnost.

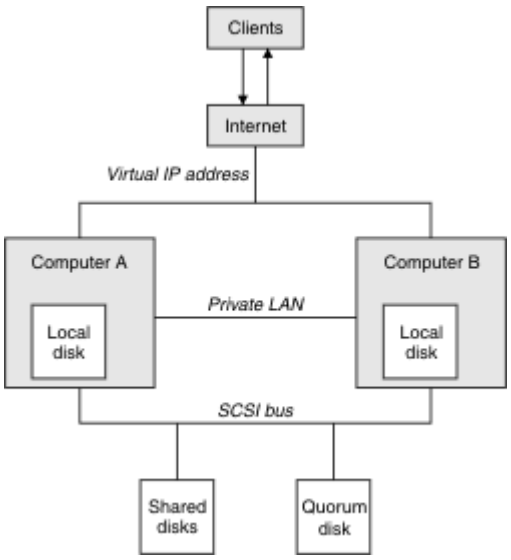
“Konfigurace vysoké dostupnosti” na stránce 429 obsahuje porovnání mezi klastry MSCS, správci front s více instancemi a klastry IBM MQ .

V této sekci a v jejích podřízených tématech výraz *cluster*, je-li používán samostatně, **vždy** znamená klastr MSCS. To je odlišné od klastru IBM MQ popsaného jinde v této příručce.

Klastr se dvěma počítači se skládá ze dvou počítačů (například A a B), které jsou společně připojeny k síti pro klientský přístup pomocí *virtuální IP adresy*. Mohou být také vzájemně propojeny pomocí jedné nebo více soukromých sítí. A a B sdílí alespoň jeden disk pro serverovou aplikaci na každé z nich. Je zde také další sdílený disk, který musí být redundantním polem nezávislých disků (*RAID*). Úroveň 1, pro výlučné použití MSCS; je to známo jako *kvorum* disk. MSCS monitoruje oba počítače, aby kontrolovalo, zda je hardware a software správně spuštěný.

V jednoduchém nastavení, jako je tento, mají oba počítače nainstalovány všechny aplikace, ale pouze počítač A běží s aktivními aplikacemi; počítač B je právě spuštěný a čeká. Pokud počítač A narazí na některou z řady problémů, služba MSCS ukončí přerušenou aplikaci řádným způsobem, přenese její stavová data na druhý počítač a znovu zahájí aplikaci. To je známé jako *překonání selhání*. Aplikace mohou být *informovaná o klastru* tak, aby plně spolupracovaly se službou MSCS a failover facefully.

Typické nastavení pro klastr se dvěma počítači je zobrazeno v části Obrázek 74 na stránce 442.



Obrázek 74. Klastr serverů MSCS se dvěma počítači

Každý počítač má přístup ke sdílenému disku, ale pouze jeden po druhém, pod kontrolou MSCS. V případě překonání selhání přepne služba MSCS přístup k jinému počítači. Samotný sdílený disk je obvykle RAID, ale nemusí být.

Každý počítač je připojen k externí síti pro klientský přístup a každý z nich má IP adresu. Avšak externí klient, komunikující s tímto klastrem, si je vědom pouze jedné *virtuální adresy IP*a služba MSCS směruje provoz IP v rámci klastru odpovídajícím způsobem.

MSCS také provádí svou vlastní komunikaci mezi oběma počítači, a to buď prostřednictvím jednoho nebo více soukromých připojení, nebo přes veřejnou síť, například k monitorování stavů pomocí prezenčního signálu a k synchronizaci svých databází.

Windows *Nastavení produktu IBM MQ pro klastrování MSCS*

Nakonfigurujte produkt IBM MQ pro klastrování tak, že převedíte správce front na jednotku MSCS (překonání selhání). Definujete správce front jako prostředek pro službu MSCS, který jej pak může monitorovat a přenést jej do jiného počítače v klastru, pokud se vyskytne problém.

Chcete-li nastavit systém pro tento systém, začněte instalací produktu IBM MQ na každém počítači v klastru.

Vzhledem k tomu, že správce front je přidružen k názvu instalace produktu IBM MQ , musí být název instalace produktu IBM MQ na všech počítačích v klastru stejný. Viz téma Instalace a odinstalace.

Samotné správce front musí existovat pouze na počítači, na kterém je vytvoříte. V případě překonání selhání iniciuje služba MSCS správce front v jiném počítači. Správci front však musí mít své soubory protokolu a datové soubory na sdíleném disku klastru, nikoli na lokální jednotce. Máte-li již správce front instalovaný na lokální jednotce, můžete jej migrovat pomocí nástroje poskytnutého s produktem IBM MQ; viz “Přesun správce front do úložiště MSCS” na stránce 445. Chcete-li vytvořit nové správce front pro použití se službou MSCS, přečtěte si téma “Vytvoření správce front pro použití se službou MSCS” na stránce 444.

Po instalaci a migraci použijte správce klastru MSCS, který bude produkt MSCS informovat o správcích front, viz “Vložení správce front do ovládacího prvku MSCS” na stránce 446.

Pokud se rozhodnete odebrat správce front z ovládacího prvku MSCS, použijte proceduru popsanou v tématu “Odebrání správce front z ovládacího prvku MSCS” na stránce 452.

Windows *Nastavit symetrii a MSCS*

Když se aplikace přepne z jednoho uzlu na druhou, musí se chovat stejným způsobem, bez ohledu na uzel. Nejlepším způsobem, jak zajistit, aby se tato prostředí shodovala.

Pokud můžete, nastavte klastr se stejným hardwarem, softwarem operačního systému, softwarem produktu a konfigurací na každém počítači. Zejména zkontrolujte, zda je veškerý požadovaný software nainstalovaný na těchto dvou počítačích identický z hlediska verze, úrovně údržby, SupportPacs, cest a uživatelských procedur a že existuje společný prostor jmen (zabezpečení ochrany dat), jak je popsáno v tématu "Zabezpečení MSCS" na stránce 443.

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 obecný obor názvů (prostředí zabezpečení) v rámci klastru.
- Nastavte uzly členů klastru MSCS na doménu, ve které je účet uživatele, který je *vlastníkem klastru* .
- Vytvořte účty ostatních uživatelů v klastru také doménové účty, aby byly k dispozici na obou uzlech. Je tomu tak automaticky, pokud již máte doménu, a účty vztahující se k IBM MQ jsou účty domény. Pokud v současné době nemáte doménu, zvažte nastavení *minidomény* , která bude určena pro uzly klastru a příslušné účty. Vaším cílem je, aby váš klastr dvou počítačů vypadá jako jediný výpočetní prostředek.

  Pamatujte na to, že účet, který je lokálně na jednom počítači, neexistuje na druhém počítači. I když vytvoříte účet se stejným názvem na druhém počítači, jeho identifikátor zabezpečení (SID) se liší, takže když se vaše aplikace přesune do jiného uzlu, oprávnění na tomto uzlu neexistují.

Během překonání selhání nebo přesunu produkt IBM MQ MSCS zajistí, aby všechny soubory, které obsahují objekty správce front, měly ekvivalentní povolení v cílovém uzlu. Explicitně, kód zkontroluje, že administrátoři a skupiny mqm a účet SYSTEM mají plnou kontrolu, a že pokud měl `Everyone` přístup pro čtení ke starému uzlu, je toto oprávnění přidáno do cílového uzlu.

K spuštění služby IBM MQ můžete použít účet domény. Ujistěte se, že existuje v lokální skupině mqm na každém počítači v klastru.

Windows *Použití více správců front se službou MSCS*

Pokud na počítači provozujete více než jednoho správce front, můžete vybrat jedno z těchto nastavení.

Nastavení jsou následující:

- Všichni správci front v jedné skupině. Pokud se v této konfiguraci vyskytne problém s libovolným správcem front, všechny správce front v rámci skupiny překoná selhání na jiný počítač jako skupinu.
- Jednotlivý správce front v každé skupině. Pokud se v této konfiguraci vyskytne problém se správcem front, dojde k selhání na jiném počítači, aniž by to mělo vliv na ostatní správce front.
- Směs prvních dvou nastavení.

Windows *Režimy klastru a MSCS*

Existují dva režimy, ve kterých můžete spustit klastrový systém s produktem IBM MQ v systému Windows: Aktivní/pasivní nebo Aktivní/Aktivní.

Poznámka: Používáte-li službu MSCS spolu se serverem Microsoft Transaction Server (COM +), nemůžete používat aktivní/aktivní režim.

Aktivní/pasivní režim

V režimu Aktivní/Pasivní režim má počítač A spuštěnou aplikaci a počítač B je záložní, používá se pouze tehdy, když MSCS zjistí problém.

Tento režim můžete použít pouze s jedním sdíleným diskem, ale pokud jakákoli aplikace způsobí překonání selhání, **všechny** aplikace musí být přeneseny jako skupina (protože přístup ke sdílenému disku může v daném okamžiku přistupovat pouze jeden počítač).

Můžete nakonfigurovat službu MSCS s hodnotou A jako s počítačem *preferováno* . Poté, je-li počítač A opraven nebo vyměněn a znovu pracuje správně, služba MSCS to zjistí a automaticky přepne aplikaci zpět na počítač A.

Pokud provozujete více než jednoho správce front, zvažte možnost samostatného sdílení se sdíleným diskem pro každý správce front. Poté umístěte každého správce front do samostatné skupiny v prostředí MSCS. Tímto způsobem může kterýkoli správce front provést překonání selhání na jiný počítač, aniž by to mělo vliv na ostatní správce front.

Aktivní/aktivní režim

V Aktivním/aktivním režimu mají počítače A a B spuštěné aplikace a skupiny na každém počítači jsou nastaveny tak, aby používaly jiný počítač jako zálohu. Pokud je na počítači A detekováno selhání, MSCS převede stavová data na počítač B a znovu iniciuje aplikaci. počítač B pak provozuje svou vlastní aplikaci a A je.

Pro toto nastavení budete potřebovat alespoň dva sdílené disky. MSCS můžete nakonfigurovat jako upřednostňovaný počítač pro aplikace A a B jako upřednostňovaný počítač pro aplikace B. Po překonání selhání a opravě se každá aplikace automaticky ukončí na svém vlastním počítači.

Pro IBM MQ to znamená, že můžete například spustit dva správce front, jeden na každém z A a B, přičemž každá z nich využívá plnou moc svého vlastního počítače. Po selhání na počítači A se oba správci front spustí na počítači B. To znamená sdílet sílu jednoho počítače se sníženou schopností zpracovávat velká množství dat při rychlosti. Vaše kritické aplikace však budou stále k dispozici, zatímco opravíte a opravíte poruchu na A.

Windows *Vytvoření správce front pro použití se službou MSCS*

Tento postup zajišťuje, že bude vytvořen nový správce front takovým způsobem, aby byl vhodný pro přípravu a umístění v rámci řízení MSCS.

Začneš tím, že vytvoříte správce front se všemi jeho prostředky na lokální jednotce a poté migrujte soubory protokolu a datové soubory na sdílený disk. (Tuto operaci můžete vrátit zpět.) **Nesnažte se** vytvořit správce front s jeho prostředky na sdílené jednotce.

Správce front pro použití se službou MSCS můžete vytvořit dvěma způsoby, buď z příkazového řádku, nebo v produktu IBM MQ Explorer. Výhodou použití příkazového řádku je to, že správce front je vytvořen *zastaveno* a nastaven na *ruční spuštění*, které je připraveno pro službu MSCS. (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 se službou MSCS, postupujte takto:

1. Ujistěte se, že máte proměnnou prostředí `MQSPREFIX` nastavenou tak, aby odkazovala na lokální jednotku, například na `C:\IBM MQ`. Pokud změníte toto nastavení, znovu zaveďte systém počítače, aby se při změně došlo k jeho změně. Pokud proměnnou nenastavíte, bude správce front vytvořen ve výchozím adresáři 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 “Přesun správce front do úložiště MSCS” na stránce 445.

Vytvoření správce front pomocí produktu IBM MQ Explorer

Následujícím postupem vytvořte správce front s použitím produktu IBM MQ Explorerpro použití se službou MSCS:

1. Spusťte IBM MQ Explorer z nabídky Start.
2. V pohledu Navigator rozbalte uzly 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 Vytvoření 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 `Start Queue Manager` a `Create Server Connection Channel` , pak klepněte na tlačítko **Další >**.
7. Dokončete dialogové okno (Krok 4) a poté klepněte na tlačítko **Dokončit**.
8. Pokračujte “Přesun správce front do úložiště MSCS” na stránce 445.

Windows *Přesun správce front do úložiště MSCS*

Tento postup nakonfiguruje existujícího správce front tak, aby byl vhodný pro vložení do řízení MSCS.

Chcete-li toho dosáhnout, přesunete soubory protokolu a datové soubory na sdílené disky a zpřístupníte je ostatním počítačům v případě selhání. Existující správce front může mít například takové cesty, jako například `C:\WebSphere MQ\log\`*QMname* a `C:\WebSphere MQ\qmgrs\`*QMname*.

Upozornění: Nepokoušejte se soubory přesunout ručně; použijte obslužný program dodávaný jako součást podpory MSCS produktu IBM MQ , jak je popsáno v tomto tématu.

Pokud přesouvaná správce front používá připojení TLS a úložiště klíčů TLS se nachází v datovém adresáři správce front na lokálním počítači, bude úložiště klíčů přesunuto spolu se zbytkem správce front na sdílený disk. Při výchozím nastavení je atribut správce front, který určuje umístění úložiště klíčů TLS, SSLKEYR, nastaven na hodnotu *MQ_INSTALLATION_PATH*`\qmgrs\QMGRNAME\ssl\key`, která se nachází pod datovým adresářem správce front. *MQ_INSTALLATION_PATH* představuje adresář vysoké úrovně, ve kterém je nainstalován produkt IBM MQ . Příkaz `hamvmqm` neupravuje tento atribut správce front. V této situaci musíte upravit atribut správce front, SSLKEYR, pomocí příkazu IBM MQ Explorer nebo příkazu MQSC `ALTER QMGR`, aby ukazoval na nový soubor úložiště klíčů TLS.

Postup je následující:

1. Ukončete činnost správce front a zkontrolujte, zda nedošlo k žádným chybám.
2. Pokud jsou soubory protokolu správce front nebo soubory fronty již uloženy na sdíleném disku, přeskočte zbývající část této procedury a pokračujte přímo na “Vložení správce front do ovládacího prvku MSCS” na stránce 446.
3. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (viz “Soubory protokolu správce front” na stránce 455 , proč je to důležité).
4. Pokud již máte vhodný prostředek sdíleného disku, pokračujte krokem 6. Jinak pomocí administrátora klastru MSCS vytvořte prostředek typu *shared disk* s dostatečnou kapacitou pro ukládání souborů protokolu správce front a datových souborů (fronty).
5. Otestujte sdílený disk pomocí administrátora klastru MSCS a přemístěte jej z jednoho uzlu klastru do druhého a znovu jej přesuňte.
6. Ujistěte se, že je sdílený disk online na uzlu klastru, kde jsou soubory protokolu správce front a datové soubory uloženy lokálně.
7. Spusťte obslužný program k přesunutí správce front následujícím způsobem:

   ```
   hamvmqm /m qmname /dd " e: \
   IBM MQ " /ld " e: \
   IBM MQ \log"
   ```

   nahrazení názvu správce front názvem *qmname*, písmeno jednotky sdíleného disku pro *e*a váš vybraný adresář pro *IBM MQ*. Adresáře se vytvoří, pokud ještě neexistují.
8. Otestujte správce front, abyste se ujistili, že pracuje, pomocí produktu IBM MQ Explorer. Příklad:

a. Klepněte pravým tlačítkem myši na uzel stromu správce front a poté vyberte volbu **Spustit**. Spustí se správce front.

b. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a poté vyberte volbu **Nový** > **Lokální fronta ...**, a pojmenujte frontu jako název.

c. Klepněte na tlačítko **Dokončit**.

d. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel Vložit testovací zprávu.

e. Zadejte nějaký text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.

f. Klepněte pravým tlačítkem myši na frontu a poté 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 poté vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.

i. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Odstranit ...**. Zobrazí se panel s potvrzením, klepněte na tlačítko **OK**. Fronta je odstraněna.

j. Klepněte pravým tlačítkem myši na uzel stromu správce front a poté vyberte volbu **Zastavit ...**. Zobrazí se panel Ukončení správce front.

k. Klepněte na tlačítko **OK**. Správce front je zastaven.

9. Jako administrátor produktu IBM MQ se ujistěte, že je atribut spuštění správce front nastaven na ruční. V poli IBM MQ Explorernastavte pole spuštění na hodnotu `manual` v panelu vlastností správce front.
10. Pokračujte “Vložení správce front do ovládacího prvku MSCS” na stránce 446.

Windows *Vložení správce front do ovládacího prvku MSCS*

Úlohy zahrnuté do umístění správce front v rámci řízení MSCS, včetně nezbytných úloh.

Před vložení správce front pod ovládací prvek MSCS

Před vložení správce front v rámci řízení MSCS proveďte následující úlohy:

1. Ujistěte se, že produkt IBM MQ a jeho podpora MSCS jsou instalovány na obou počítačích v klastru a že software na každém počítači je identický, jak je popsáno v “Nastavení produktu IBM MQ pro klastrování MSCS” na stránce 442.
2. Obslužný program **haregtyp** použijte k registraci IBM MQ jako typu prostředku MSCS na všech uzlech klastru. Další informace naleznete v dokumentu “Podpora obslužných programů MSCS” na stránce 456 .
3. Pokud jste správce front dosud nevytvořili, přečtěte si téma “Vytvoření správce front pro použití se službou MSCS” na stránce 444.
4. Pokud jste správce front vytvořili nebo již existuje, ujistěte se, že jste provedli proceduru v produktu “Přesun správce front do úložiště MSCS” na stránce 445.
5. Zastavte správce front, je-li spuštěný, a to buď pomocí příkazového řádku, nebo pomocí Průzkumníka IBM MQ .
6. Před přechodem na následující procedury produktu Windows v tomto tématu proveďte test operací MSCS sdílených jednotek.

Windows Server 2012

Chcete-li umístit správce front v rámci řízení MSCS na server Windows Server 2012, použijte následující postup:

1. Přihlaste se k počítači uzlu klastru, který je hostitelem správce front, nebo se přihlaste ke vzdálené pracovní stanici jako uživatel s oprávněním k administraci klastru a připojte se k uzlu klastru, který je hostitelem správce front.
2. Spusťte nástroj Správa klastru pro překonání selhání.
3. Klepněte pravým tlačítkem myši na **Správa klastru pro překonání selhání > Připojit klastr ...** k otevření připojení ke klastru.
4. Na rozdíl od schématu skupiny, které se používá v produktu MSCS Cluster Administrator na předchozích verzích produktu Windows, používá nástroj pro správu klastru pro překonání selhání koncepci služeb a aplikací. Konfigurovaná služba nebo aplikace obsahuje všechny prostředky nezbytné pro klastrování jedné aplikace. Správce front v prostředí MSCS lze konfigurovat takto:
   a. Klepněte pravým tlačítkem myši na klastr a vyberte volbu **Konfigurovat roli** , chcete-li spustit průvodce konfigurací.
   b. Vyberte volbu **Jiný server** na panelu "Vybrat službu nebo aplikaci".
   c. Vyberte příslušnou adresu IP jako přístupový bod klienta.

      Tato adresa by měla být nepoužívanou adresou IP, která má být použita klienty a dalšími správci front pro připojení ke správci front *virtual* . Tato adresa IP není normální (statická) adresa uzlu. Jedná se o přídavnou adresu, která je mezi nimi *floats* . Ačkoli služba MSCS zpracovává směrování této adresy, **neověřuje** , zda je adresa dosažitelná.
   d. Přiřaďte úložné zařízení pro výhradní použití správcem front. Toto zařízení musí být vytvořeno jako instance prostředku, než bude možné je přiřadit.

      K ukládání protokolů a souborů fronty můžete použít jednu jednotku, nebo můžete tyto soubory rozdělit na více jednotek. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, se ujistěte, že všechny jednotky použité tímto správcem front jsou pro tohoto správce front výhradní, to znamená, že nic jiného nespoléhá na jednotky. Také se ujistěte, že vytváříte instanci prostředku pro každou jednotku, kterou správce front používá.

      Typ prostředku pro jednotku závisí na podpoře SCSI, kterou používáte; podívejte se na instrukce k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte ji ze své aktuální skupiny do té, která byla vytvořena pro správce front.

      Pro každý prostředek jednotky nastavte možné vlastníky na obou uzlech. Nastavit závislé prostředky na žádné.
   e. Vyberte prostředek **MQSeries MSCS** na panelu "Vybrat typ prostředku".
   f. Proveďte zbývající kroky v průvodci.
5. Před přivedení prostředku do režimu online potřebuje prostředek MSCS produktu MQSeries další konfiguraci:
   a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'Nová MSCS MQSeries'.
   b. Klepněte pravým tlačítkem myši na položku **Vlastnosti** v prostředku MQ .
   c. Konfigurujte prostředek:
      - `Name` ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
      - `Run in a separate Resource Monitor` ; pro lepší izolaci
      - `Possible owners` ; nastavit oba uzly
      - `Dependencies` ; Přidejte jednotku a adresu IP pro tohoto správce front.

        Varování: Selhání při přidávání těchto závislostí znamená, že produkt IBM MQ se pokusí zapsat stav správce front na chybný disk klastru během překonání selhání. Vzhledem k tomu, že se mnoho procesů může pokusit o zápis na tento disk současně, některé procesy IBM MQ mohou být zablokovány ze spuštění.
      - `Parameters` ; takto:

- `QueueManagerName` (povinné); název správce front, kterého má tento prostředek řídit. Tento správce front musí existovat na lokálním počítači.
- `PostOnlineCommand` (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz "Příkaz PostOnlinea příkaz PreOfflinev prostředí MSCS" na stránce 456.
- `PreOfflineCommand` (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu online na offline. Další podrobnosti viz "Příkaz PostOnlinea příkaz PreOfflinev prostředí MSCS" na stránce 456.

  Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 60000 ms. Tyto výchozí hodnoty lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz "Systém výzev looksAlive a isAlive na MSCS" na stránce 452.

d. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu "Použití preferovaných uzlů v MSCS" na stránce 456).

e. *Zásada pro překonání selhání* je standardně nastavena na citlivé hodnoty, ale můžete vyladit prahové hodnoty a období, které řídí *překonání selhání prostředků* a *Překonání selhání skupiny* tak, aby odpovídaly zavedům umístěným na správci front.

6. Otestujte správce front tím, že jej otevřete online v produktu MSCS Cluster Administrator a vystavujete jej testovací pracovní zátěži. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM MQ . Příklad:

   a. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a poté vyberte volbu **Nový** > **Lokální fronta ...**, a pojmenujte frontu jako název.

   b. Klepněte na tlačítko **Dokončit**. Fronta se vytvoří a zobrazí se v zobrazení obsahu.

   c. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel Vložit testovací zprávu.

   d. Zadejte nějaký text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.

   e. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Procházet zprávy ...**. Zobrazí se panel Prohlížeč zpráv.

   f. Ujistěte se, že vaše zpráva je ve frontě, a klepněte na tlačítko **Zavřít**. Panel Prohlížeč zpráv se zavře.

   g. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.

   h. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Odstranit ...**. Zobrazí se panel s potvrzením, klepněte na tlačítko **OK**. Fronta je odstraněna.

7. Otestujte, zda lze správce front převést do stavu offline a zpět online pomocí administrátora klastru MSCS.

8. Simulovat překonání selhání.

   V Administrátorovi klastru MSCS klepněte pravým tlačítkem myši na skupinu obsahující správce front a vyberte volbu `Move Group`. To může trvat několik minut. (Pokud chcete rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části "Přesun správce front do úložiště MSCS" na stránce 445.) Můžete také klepnout pravým tlačítkem myši a vybrat `Initiate Failure` ; Akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows Server 2008

Chcete-li umístit správce front v rámci řízení MSCS na server Windows Server 2008, postupujte takto:

1. Přihlaste se k počítači uzlu klastru, který je hostitelem správce front, nebo se přihlaste ke vzdálené pracovní stanici jako uživatel s oprávněním k administraci klastru a připojte se k uzlu klastru, který je hostitelem správce front.
2. Spusťte nástroj Správa klastru pro překonání selhání.

3. Klepněte pravým tlačítkem myši na **Správa klastru pro překonání selhání > Spravovat klastr ...** k otevření připojení ke klastru.
4. Na rozdíl od schématu skupiny, které se používá v produktu MSCS Cluster Administrator na předchozích verzích produktu Windows, používá nástroj pro správu klastru pro překonání selhání koncepci služeb a aplikací. Konfigurovaná služba nebo aplikace obsahuje všechny prostředky nezbytné pro klastrování jedné aplikace. Správce front v prostředí MSCS lze konfigurovat takto:
   a. Klepněte pravým tlačítkem myši na **Služby a aplikace > Konfigurovat službu nebo aplikaci ...** a spusťte průvodce konfigurací.
   b. Vyberte volbu **Další server** na panelu **Vybrat službu nebo aplikaci** .
   c. Vyberte příslušnou adresu IP jako přístupový bod klienta.

      Tato adresa by měla být nepoužívanou adresou IP, která má být použita klienty a dalšími správci front pro připojení ke správci front *virtual* . Tato adresa IP není normální (statická) adresa uzlu. Jedná se o přídavnou adresu, která je mezi nimi *floats* . Ačkoli služba MSCS zpracovává směrování této adresy, **neověřuje** , zda je adresa dosažitelná.
   d. Přiřaďte úložné zařízení pro výhradní použití správcem front. Toto zařízení musí být vytvořeno jako instance prostředku, než bude možné je přiřadit.

      K ukládání protokolů a souborů fronty můžete použít jednu jednotku, nebo můžete tyto soubory rozdělit na více jednotek. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, se ujistěte, že všechny jednotky použité tímto správcem front jsou pro tohoto správce front výhradní, to znamená, že nic jiného nespoléhá na jednotky. Také se ujistěte, že vytváříte instanci prostředku pro každou jednotku, kterou správce front používá.

      Typ prostředku pro jednotku závisí na podpoře SCSI, kterou používáte; podívejte se na instrukce k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte ji ze své aktuální skupiny do té, která byla vytvořena pro správce front.

      Pro každý prostředek jednotky nastavte možné vlastníky na obou uzlech. Nastavit závislé prostředky na žádné.
   e. Vyberte prostředek **MQSeries MSCS** na panelu **Výběr typu prostředku** .
   f. Proveďte zbývající kroky v průvodci.
5. Před přivedení prostředku do režimu online potřebuje prostředek MSCS produktu MQSeries další konfiguraci:
   a. Vyberte nově definovanou službu, která obsahuje prostředek s názvem 'Nová MSCS MQSeries'.
   b. Klepněte pravým tlačítkem myši na položku **Vlastnosti** v prostředku MQ .
   c. Konfigurujte prostředek:
      - `Name` ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
      - `Run in a separate Resource Monitor` ; pro lepší izolaci
      - `Possible owners` ; nastavit oba uzly
      - `Dependencies` ; Přidejte jednotku a adresu IP pro tohoto správce front.

        Varování: Selhání při přidávání těchto závislostí znamená, že produkt IBM MQ se pokusí zapsat stav správce front na chybný disk klastru během překonání selhání. Vzhledem k tomu, že se mnoho procesů může pokusit o zápis na tento disk současně, některé procesy IBM MQ mohou být zablokovány ze spuštění.
      - `Parameters` ; takto:
        – `QueueManagerName` (povinné); název správce front, kterého má tento prostředek řídit. Tento správce front musí existovat na lokálním počítači.
        – `PostOnlineCommand` (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz “Příkaz PostOnlinea příkaz PreOfflinev prostředí MSCS” na stránce 456.

– `PreOfflineCommand` (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu online na offline. Další podrobnosti viz "Příkaz PostOnlinea příkaz PreOfflinev prostředí MSCS" na stránce 456.

Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 60000 ms. Tyto výchozí hodnoty lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz "Systém výzev looksAlive a isAlive na MSCS" na stránce 452.

d. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu "Použití preferovaných uzlů v MSCS" na stránce 456).

e. *Zásada pro překonání selhání* je standardně nastavena na citlivé hodnoty, ale můžete vyladit prahové hodnoty a období, které řídí *překonání selhání prostředků* a *Překonání selhání skupiny* tak, aby odpovídaly zavedům umístěným na správci front.

6. Otestujte správce front tím, že jej otevřete online v produktu MSCS Cluster Administrator a vystavujete jej testovací pracovní zátěži. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM MQ . Příklad:

a. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a poté vyberte volbu **Nový** > **Lokální fronta ...**, a pojmenujte frontu jako název.

b. Klepněte na tlačítko **Dokončit**. Fronta se vytvoří a zobrazí se v zobrazení obsahu.

c. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel **Vložit testovací zprávu** .

d. Zadejte nějaký text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.

e. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Procházet zprávy ...**. Zobrazí se panel **Prohlížeč zpráv** .

f. Ujistěte se, že vaše zpráva je ve frontě, a klepněte na tlačítko **Zavřít**. Panel **Prohlížeč zpráv** se zavře.

g. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.

h. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Odstranit ...**. Zobrazí se panel s potvrzením, klepněte na tlačítko **OK**. Fronta je odstraněna.

7. Otestujte, zda lze správce front převést do stavu offline a zpět online pomocí administrátora klastru MSCS.

8. Simulovat překonání selhání.

V Administrátorovi klastru MSCS klepněte pravým tlačítkem myši na skupinu obsahující správce front a vyberte volbu `Move Group`. To může trvat několik minut. (Pokud chcete rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části "Přesun správce front do úložiště MSCS" na stránce 445.) Můžete také klepnout pravým tlačítkem myši a vybrat `Initiate Failure` ; Akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows 2003

Chcete-li umístit správce front do řízení MSCS na serveru Windows 2003, použijte následující postup:

1. Přihlaste se k počítači uzlu klastru, který je hostitelem správce front, nebo se přihlaste ke vzdálené pracovní stanici jako uživatel s oprávněním k administraci klastru a připojte se k uzlu klastru, který je hostitelem správce front.

2. Spusťte administrátora klastru MSCS.

3. Otevřete připojení ke klastru.

4. Vytvořte skupinu MSCS, která má být použita k uchování prostředků pro správce front. Pojmenujte skupinu takovým způsobem, že je zřejmé, ke kterému správci front se vztahuje. Každá skupina může obsahovat více správců front, jak je popsáno v tématu "Použití více správců front se službou MSCS" na stránce 443.

Použijte skupinu pro všechny zbývající kroky.

5. Vytvořte instanci prostředku pro každou logickou jednotku SCSI, kterou používá správce front.

   K ukládání protokolů a souborů fronty můžete použít jednu jednotku, nebo můžete tyto soubory rozdělit na více jednotek. V obou případech, pokud má každý správce front svůj vlastní sdílený disk, se ujistěte, že všechny jednotky použité tímto správcem front jsou pro tohoto správce front výhradní, to znamená, že nic jiného nespoléhá na jednotky. Také se ujistěte, že vytváříte instanci prostředku pro každou jednotku, kterou správce front používá.

   Typ prostředku pro jednotku závisí na podpoře SCSI, kterou používáte; podívejte se na instrukce k adaptéru SCSI. Pro každou ze sdílených jednotek již mohou existovat skupiny a prostředky. Pokud ano, nemusíte vytvářet instanci prostředku pro každou jednotku. Přesuňte ji ze své aktuální skupiny do té, která byla vytvořena pro správce front.

   Pro každý prostředek jednotky nastavte možné vlastníky na obou uzlech. Nastavit závislé prostředky na žádné.

6. Vytvořte instanci prostředku pro adresu IP.

   Vytvořte prostředek adresy IP (typ prostředku *IP adresa*). Tato adresa by měla být nepoužívanou adresou IP, která má být použita klienty a dalšími správci front pro připojení ke správci front *virtual* . Tato adresa IP není normální (statická) adresa uzlu. Jedná se o přídavnou adresu, která je mezi nimi *floats* . Ačkoli služba MSCS zpracovává směrování této adresy, **neověřuje** , zda je adresa dosažitelná.

7. Vytvořte instanci prostředku pro správce front.

   Vytvořte prostředek typu *IBM MQ MSCS*. Průvodce vás vyzve k zadání různých položek, včetně následujících:

   - `Name` ; Vyberte název, který usnadňuje identifikaci správce front, pro kterého je určen.
   - `Add to group` ; použijte skupinu, kterou jste vytvořili
   - `Run in a separate Resource Monitor` ; pro lepší izolaci
   - `Possible owners` ; nastavit oba uzly
   - `Dependencies` ; Přidejte jednotku a adresu IP pro tohoto správce front.

     Varování: Selhání při přidávání těchto závislostí znamená, že produkt IBM MQ se pokusí zapsat stav správce front na chybný disk klastru během překonání selhání. Vzhledem k tomu, že se mnoho procesů může pokusit o zápis na tento disk současně, některé procesy IBM MQ mohou být zablokovány ze spuštění.

   - `Parameters` ; takto:
     - `QueueManagerName` (povinné); název správce front, kterého má tento prostředek řídit. Tento správce front musí existovat na lokálním počítači.
     - `PostOnlineCommand` (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu offline na online. Další podrobnosti viz “Příkaz PostOnlinea příkaz PreOfflinev prostředí MSCS” na stránce 456.
     - `PreOfflineCommand` (volitelné); můžete zadat program, který se má spustit vždy, když prostředek správce front změní svůj stav z režimu online na offline. Další podrobnosti viz “Příkaz PostOnlinea příkaz PreOfflinev prostředí MSCS” na stránce 456.

       Poznámka: Interval výzev *looksAlive* je nastaven na výchozí hodnotu 5000 ms. Interval výzev *isAlive* je nastaven na výchozí hodnotu 30000 ms. Tyto výchozí hodnoty lze upravit pouze po dokončení definice prostředku. Další podrobnosti viz “Systém výzev looksAlive a isAlive na MSCS” na stránce 452.

8. Volitelně nastavte upřednostňovaný uzel (ale poznamenejte si komentáře v produktu “Použití preferovaných uzlů v MSCS” na stránce 456).
9. *Zásada překonání selhání* (definovaná ve vlastnostech skupiny) je standardně nastavena na citlivé hodnoty, ale můžete vyladit prahové hodnoty a období, které řídí *překonání selhání prostředků* a *Překonání selhání skupiny* tak, aby odpovídaly zátěži umístěné ve správci front.

10. Otestujte správce front tím, že jej otevřete online v produktu MSCS Cluster Administrator a vystavujete jej testovací pracovní zátěži. Pokud experimentujete se správcem testovací fronty, použijte Průzkumníka IBM MQ . Příklad:
    a. Klepněte pravým tlačítkem myši na uzel stromu `Fronty` a poté vyberte volbu **Nový** > **Lokální fronta ...**, a pojmenujte frontu jako název.
    b. Klepněte na tlačítko **Dokončit**. Fronta se vytvoří a zobrazí se v zobrazení obsahu.
    c. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Vložit testovací zprávu ...**. Zobrazí se panel **Vložit testovací zprávu** .
    d. Zadejte nějaký text zprávy, poté klepněte na volbu **Vložit testovací zprávu**a zavřete panel.
    e. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Procházet zprávy ...**. Zobrazí se panel **Prohlížeč zpráv** .
    f. Ujistěte se, že vaše zpráva je ve frontě, a klepněte na tlačítko **Zavřít**. Panel **Prohlížeč zpráv** se zavře.
    g. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Vymazat zprávy ...**. Zprávy ve frontě jsou vymazány.
    h. Klepněte pravým tlačítkem myši na frontu a poté vyberte volbu **Odstranit ...**. Zobrazí se panel s potvrzením, klepněte na tlačítko **OK**. Fronta je odstraněna.
11. Otestujte, zda lze správce front převést do stavu offline a zpět online pomocí administrátora klastru MSCS.
12. Simulovat překonání selhání.

    V Administrátorovi klastru MSCS klepněte pravým tlačítkem myši na skupinu obsahující správce front a vyberte volbu `Move Group`. To může trvat několik minut. (Pokud chcete rychle přesunout správce front do jiného uzlu, postupujte podle pokynů v části “Přesun správce front do úložiště MSCS” na stránce 445.) Můžete také klepnout pravým tlačítkem myši a vybrat `Initiate Failure` ; Akce (lokální restartování nebo překonání selhání) závisí na aktuálním stavu a nastavení konfigurace.

Windows *Systém výzev looksAlive a isAlive na MSCS*

looksAlive a *isAlive* jsou intervaly, kdy volání MSCS vrací zpět do typů prostředků a požaduje, aby prostředek provedl kontrolu, aby určil vlastní provozní stav. To v konečném důsledku určuje, zda se MSCS pokusí o překonání selhání prostředku.

Při každé příležitosti, kdy vyprší interval *looksAlive* (výchozí 5000 ms), je prostředek správce front volán, aby provedl svou vlastní kontrolu, aby určil, zda je jeho stav uspokojivý.

Při každé příležitosti, kdy vyprší interval *isAlive* (výchozí hodnota 30000 ms), je pro prostředek správce front provedeno další volání k provedení další kontroly, aby bylo možné určit, zda prostředek správně funguje. To umožňuje dvě úrovně kontroly typů prostředků.

1. Kontrola stavu *looksAlive* se má zjistit, zda se prostředek jeví jako funkční.
2. Významnější kontrola *isAlive* , která určuje, zda je prostředek správce front aktivní.

Je-li prostředek správce front určen jako neaktivní, MSCS na základě dalších rozšířených voleb MSCS spustí překonání selhání pro prostředek a přidružené závislé prostředky na jiném uzlu v klastru. Další informace naleznete v tématu Dokumentace MSCS.

Windows *Odebrání správce front z ovládacího prvku MSCS*

Správce front můžete odebrat z ovládacího prvku MSCS a vrátit je do ruční administrace.

Odebrání správců front z ovládacího prvku MSCS pro operace údržby není nutné. Můžete to provést tak, že správce front MSCS dočasně, a to tak, že použijete administrátora klastru MSCS. Odebrání správce front z řízení MSCS je trvalejší změna. Pouze pokud se rozhodnete, že nechcete, aby MSCS měl další kontrolu nad správcem front, stačí ji již nadále měnit.

Je-li správce front odebírán pomocí připojení TSL, musíte upravit atribut správce front, SSLKEYR, pomocí Průzkumníka IBM MQ nebo příkazu MQSC `ALTER QMGR`, aby ukazoval na soubor úložiště klíčů TLS v lokálním adresáři.

Postup je:

1. Převeďte prostředek správce front do stavu offline pomocí administrátora klastru MSCS, jak je popsáno v tématu “Převedení správce front do režimu offline z prostředí MSCS” na stránce 453 .
2. Zlikvidovat instanci prostředku. Tím nedojde ke zničení správce front.
3. Volitelně proveďte migraci souborů správce front zpět ze sdílených jednotek na lokální jednotky. Chcete-li to provést, viz “Vrácení správce front z úložiště MSCS” na stránce 453.
4. Otestujte správce front.

Převedení správce front do režimu offline z prostředí MSCS

Chcete-li správce front převést do stavu offline z prostředí MSCS, proveďte následující kroky:

1. Spusťte administrátora klastru MSCS.
2. Otevřete připojení ke klastru.
3. Vyberte položku `Groups`nebo `Role` , pokud používáte produkt Windows 2012, a otevřete skupinu obsahující správce front, který má být přesunut.
4. Vyberte prostředek správce front.
5. Klepněte na něj pravým tlačítkem myši a vyberte volbu `Offline`.
6. Čekejte na dokončení.

Vrácení správce front z úložiště MSCS

Tento postup nakonfiguruje správce front tak, aby se vrátil zpět na lokální diskovou jednotku počítače, tj. stane se *normálním* správcem front IBM MQ . Chcete-li toho dosáhnout, přesuňte soubory protokolu a datové soubory ze sdílených disků. Existující správce front může mít například takové cesty, jako například `E:\WebSphere MQ\log\`*`QMname`* a `E:\WebSphere MQ\qmgrs\`*`QMname`*. Nepokoušejte se soubory přesunout ručně; pomocí obslužného programu **hamvmqm** dodávaného jako součást podpory MSCS produktu IBM MQ postupujte takto:

1. Vytvořte úplnou zálohu souborů fronty a souborů protokolu a uložte zálohu na bezpečném místě (viz “Soubory protokolu správce front” na stránce 455 , proč je to důležité).
2. Rozhodněte se, kterou lokální jednotku chcete použít, a ujistěte se, že má dostatečnou kapacitu pro ukládání souborů protokolu správce front a datových souborů (fronty).
3. Ujistěte se, že sdílený disk, na kterém jsou momentálně umístěny soubory, je online na uzlu klastru, do kterého se má přesunout protokol správce front a datové soubory.
4. Spusťte obslužný program k přesunutí správce front následujícím způsobem:

   ```
   hamvmqm /m qmname /dd " c:\
   IBM MQ " /ld "c:\
   IBM MQ \log"
   ```

   nahrazení názvu správce front *qmname*, písmeno vaší lokální diskové jednotky pro *c*a vámi zvolený adresář pro *IBM MQ* (adresáře jsou vytvořeny, pokud ještě neexistují).
5. Otestujte správce front a ujistěte se, že pracuje (jak je popsáno v tématu “Přesun správce front do úložiště MSCS” na stránce 445).

Windows *Rady a tipy pro použití MSCS*

Tento oddíl obsahuje některé obecné informace, které vám pomohou efektivně využívat podporu produktu IBM MQ pro službu MSCS.

Tento oddíl obsahuje některé obecné informace, které vám pomohou efektivně využívat podporu produktu IBM MQ pro službu MSCS.

Jak dlouho trvá, než se správce front nezdaří z jednoho počítače na druhý? Závisí to na objemu pracovní zátěže ve správci front a na mísení provozu, například o tom, jak velká část je trvalá, v rámci synchronizačního bodu a jak velká část byla potvrzena před selháním. IBM testů failover a failback time of about a minute. To bylo na velmi lehce zatíženém správci front a skutečné časy se značně liší v závislosti na zatížení.

Windows *Ověření, že MSCS pracuje*

Postupujte takto, abyste se ujistili, že máte spuštěný klastr MSCS.

Popisy úloh začínající řetězcem “Vytvoření správce front pro použití se službou MSCS” na stránce 444 předpokládají, že máte spuštěný klastr MSCS, v rámci kterého můžete vytvářet, migrovat a odstraňovat prostředky. Chcete-li se ujistit, že máte takový klastr:

1. Pomocí administrátora klastru MSCS vytvořte skupinu.
2. V rámci této skupiny vytvořte instanci generického prostředku aplikace a zadejte systémové hodiny (název cesty `C:\winnt\system32\clock.exe` a pracovní adresář produktu `C:\`).
3. Ujistěte se, že můžete prostředek převést online, že můžete přesunout skupinu, která ji obsahuje, do jiného uzlu, a že můžete prostředek převést do stavu offline.

Windows *Ruční spuštění a MSCS*

Pro správce front spravovaného pomocí MSCS je třeba nastavit atribut spuštění na ruční. Tím je zajištěno, že podpora serveru IBM MQ MSCS může restartovat službu MQSeries bez okamžitého spouštění správce front.

Podpora produktu IBM MQ MSCS musí být schopna restartovat službu, aby mohla provádět monitorování a řízení, ale sama musí zůstat v řízení, které správci front jsou spuštěny a na kterých počítačích. Další informace viz “Přesun správce front do úložiště MSCS” na stránce 445.

Windows *MSCS a správce front*

Aspekty týkající se správců front při použití MSCS.

Vytvoření odpovídajícího správce front v jiném uzlu

Chcete-li klastrování pracovat s produktem IBM MQ, potřebujete stejného správce front v uzlu B pro každý uzel na uzlu A. Avšak, nemusíte výslovně vytvářet druhou. Správce front můžete vytvořit nebo připravit na jednom uzlu, přesunout jej do jiného uzlu, jak je popsáno v tématu “Přesun správce front do úložiště MSCS” na stránce 445, a je na daném uzlu plně duplikován.

Výchozí správci front

V rámci ovládacího prvku MSCS nepoužívejte výchozího správce front. Správce front nemá vlastnost, která z něj činí výchozí hodnotu; produkt IBM MQ uchovává svůj vlastní samostatný záznam. Přesunete-li sadu správců front jako výchozí nastavení na jiný počítač v případě překonání selhání, nestane se výchozí hodnotou. Upravte všechny aplikace tak, aby odkazovaly na specifické správce front podle názvu.

Odstranění správce front

Jakmile má správce front přesunutý uzel, jeho podrobnosti existují v registru na obou počítačích. Chcete-li jej odstranit, proveďte to jako normální na jednom počítači a poté spusťte obslužný program popsaný v tématu “Podpora obslužných programů MSCS” na stránce 456 , abyste vyčistili registr na jiném počítači.

Podpora pro existující správce front

Existující správce front můžete umístit pod ovládací prvek MSCS za předpokladu, že můžete umístit soubory protokolu správce front a soubory fronty na disk, který se nachází na sdílené sběrnici SCSI mezi

dvěma počítači (viz Obrázek 74 na stránce 442). Při vytvoření prostředku MSCS je třeba správce front krátce převést do stavu offline.

Chcete-li vytvořit nového správce front, vytvořte jej nezávisle na serveru MSCS, otestujte jej a poté jej umístěte pod ovládací prvek MSCS. Viz:

- “Vytvoření správce front pro použití se službou MSCS” na stránce 444
- “Přesun správce front do úložiště MSCS” na stránce 445
- “Vložení správce front do ovládacího prvku MSCS” na stránce 446

Vykazování MSCS, které správci front mají spravovat

Vybíráte, kteří správci front jsou umístěními pod řízením MSCS, pomocí administrátora klastru MSCS, aby bylo možné vytvořit instanci prostředku pro každého takového správce front. Tento proces vám předkládá seznam prostředků, ze kterých chcete vybrat správce front, kterého chcete spravovat.

Soubory protokolu správce front

Přesunete-li správce front do úložiště MSCS, přesunete jeho protokol a datové soubory na sdílený disk (viz příklad “Přesun správce front do úložiště MSCS” na stránce 445).

Před přesunem je vhodné správce front řádně vypnout a provést úplné zálohování datových souborů a souborů protokolu.

Více správců front

Podpora MSCS produktu IBM MQ vám umožňuje spouštět více správců front v každém počítači a umísťovat jednotlivé správce front v rámci řízení MSCS.

Windows *Vždy použít službu MSCS pro správu klastrů*

Nepokoušejte se provádět operace spuštění a zastavení přímo na libovolném správci front pod kontrolou MSCS pomocí řídicích příkazů nebo pomocí IBM MQ Explorer. Místo toho použijte administrátora klastru MSCS k převedení správce front do režimu online nebo jej převeďte do stavu offline.

Použití programu MSCS Cluster Administrator je částečně zamezené případným nejasnostem způsobenému hlášením MSCS, že je správce front offline, kdy jste jej spustili mimo kontrolu prostředí MSCS. Přesněji řečeno, zastavení správce front bez použití serveru MSCS bylo zjištěno serverem MSCS jako selhání, čímž se iniciuje překonání selhání na jiný uzel.

Windows *Práce v aktivním/aktivním režimu v MSCS*

Oba počítače v klastru MSCS mohou spouštět správce front v aktivním/aktivním režimu. Nemusíte mít plně nečinný počítač fungující jako záložní (ale pokud chcete, můžete, pokud chcete, v režimu Aktivní/Pasivní režim).

Plánujete-li používat ke spouštění pracovní zátěže oba stroje, poskytněte každému s dostatečnou kapacitou (procesor, paměť, sekundární paměť), aby se na uspokojivé úrovni výkonu spouštěla celková pracovní zátěž klastru.

Poznámka: Používáte-li službu MSCS spolu se serverem Microsoft Transaction Server (COM +), **nelze** použít režim aktivní/aktivní. Je tomu tak proto, že pro použití produktu IBM MQ s MSCS a COM +:

- Komponenty aplikace, které používají podporu COM + IBM MQ , musí být spuštěny na stejném počítači jako koordinátor distribuovaných transakcí (DTC), část COM +.
- Správce front musí být také spuštěn na stejném počítači.
- DTC musí být konfigurována jako prostředek MSCS, a proto může být spuštěna na jednom z počítačů v klastru kdykoli.

Windows *Příkaz PostOnlinea příkaz PreOfflinev prostředí MSCS*

Tyto příkazy použijte k integraci podpory MSCS produktu IBM MQ s jinými systémy. Můžete je použít k vydání příkazu IBM MQ , některá omezení wih.

Určete tyto příkazy v parametrech pro prostředek typu `IBM MQ MSCS`. Můžete je použít k integraci podpory MSCS produktu IBM MQ s jinými systémy nebo procedurami. Můžete například zadat název programu, který odesílá poštovní zprávu, aktivuje pager nebo vygeneruje nějakou jinou formu výstrahy, která má být zachycována jiným systémem monitorování.

Příkaz PostOnlineje vyvolán, když se prostředek změní z režimu offline do režimu online; příkaz PreOfflineje vyvolán pro změnu z režimu online do režimu offline. Při vyvolání jsou tyto příkazy spouštěny standardně ze systémového adresáře Windows . Protože IBM MQ používá 32bitový proces monitorování prostředků, na 64bitových systémech Windows se jedná o adresář `\Windows\SysWOW64` spíše než na adresář `\Windows\system32` . Další informace naleznete v dokumentaci produktu Microsoft o přesměrování souboru v prostředí Windows x64 . Oba příkazy běží pod uživatelským účtem, který se používá ke spuštění služby MSCS, a jsou vyvoláni asynchronně; IBM MQ podpora MSCS nečeká na dokončení zpracování, než bude pokračovat. Tím vyloučíte jakékoli riziko, že by mohly blokovat nebo zpožďovat další operace klastru.

Tyto příkazy můžete také použít k vydání příkazů IBM MQ , například k restartování žadatelských kanálů. Příkazy se však spouštějí v daném okamžiku, kdy se změní stav správce front, takže nejsou určeny k provádění dlouhodobě spuštěných funkcí a nesmí vytvářet předpoklady o aktuálním stavu správce front; je zcela možné, že ihned po uvedení správce front do stavu online administrátor vydal příkaz offline.

Chcete-li spouštět programy, které závisí na stavu správce front, zvažte vytvoření instancí typu prostředku `MSCS Generic Application` , jejich umístění do stejné skupiny MSCS jako prostředek správce front a jejich zpřístupnění v závislosti na prostředku správce front.

Windows *Použití preferovaných uzlů v MSCS*

Může být užitečný při použití aktivního/aktivního režimu v MSCS pro konfiguraci *upřednostňovaného uzlu* pro každého správce front. Obecně je však lepší nenastavit upřednostňovaný uzel, ale spoléhat se na ruční odvolání při selhání.

Na rozdíl od jiných relativně nestavových prostředků může správce front provést převedení z jednoho uzlu na druhý uzel (nebo zpět). Chcete-li se vyhnout zbytečným výpadkům, otestujte obnovený uzel předtím, než k němu dojde k selhání správce front. Toto znemožňuje použití nastavení odvolání při selhání `immediate` . Můžete nakonfigurovat návrat po selhání, aby se vyskytli mezi určitými časy dne.

Nejbezpečnější cestou je pravděpodobně přesunout správce front zpět ručně do požadovaného uzlu, když jste si jisti, že uzel je zcela obnoven. Toto vylučuje použití volby `preferred node` .

Windows *Chyby COM + při instalaci na MSCS*

Při instalaci produktu IBM MQ v nově nainstalovaném klastru MSCS může být nalezena chyba se zdrojem COM + a ID události 4691, hlášeným v protokolu událostí aplikace.

To znamená, že se pokoušíte spustit produkt IBM MQ v prostředí serveru Microsoft Cluster Server (MSCS), když se Microsoft Distributed Transaction Coordinator (MSDTC) nekonfiguroval tak, aby se spouštěl v takovém prostředí. Informace o konfiguraci produktu MSDTC v klastrovaném prostředí najdete v dokumentaci produktu Microsoft .

Windows *Podpora obslužných programů MSCS*

Seznam podpory IBM MQ pro obslužné programy MSCS, které můžete spustit na příkazovém řádku.

Podpora produktu IBM MQ pro službu MSCS zahrnuje následující obslužné programy:

Registrace/zrušení registrace typu prostředku

`haregtyp.exe`

Po *zrušení registrace* typu prostředku IBM MQ MSCS již nebudete moci vytvářet žádné prostředky tohoto typu. MSCS vám nezruší registraci typu prostředku, pokud stále máte instance tohoto typu v klastru:

1. Pomocí správce klastrů MSCS zastavte všechny správce front, kteří jsou spuštěni v rámci řízení MSCS, tak, že je budete v režimu offline, jak je popsáno v tématu “Převedení správce front do režimu offline z prostředí MSCS” na stránce 453.
2. Pomocí administrátora klastru MSCS odstraňte instance prostředků.
3. Na příkazovém řádku zrušte registraci tohoto typu prostředku zadáním následujícího příkazu:

```
haregtyp /u
```

Chcete-li *registrovat* typ (nebo jej znovu zaregistrovat později), zadejte na příkazový řádek následující příkaz:

```
haregtyp /r
```

Po úspěšné registraci knihoven MSCS je třeba restartovat systém, pokud jste tak neučinili od instalace produktu IBM MQ.

Přesunout správce front do úložiště MSCS

`hamvmqm.exe`

Viz “Přesun správce front do úložiště MSCS” na stránce 445.

Odstranit správce front z uzlu

`hadltmqm.exe`

Předpokládejme případ, kdy jste ve svém klastru měli správce front, byl přesunut z jednoho uzlu do jiného uzlu a nyní jej chcete zničit. Použijte program Průzkumník IBM MQ k jeho odstranění na uzlu, kde aktuálně je. Položky registru pro ni stále existují na jiném počítači. Chcete-li je odstranit, zadejte na příkazový řádek v tomto počítači následující příkaz:

```
hadltmqm /m qmname
```

kde `qmname` je název správce front, který má být odebrán.

Podrobnosti o nastavení kontroly a uložení

`amqmsysn.exe`

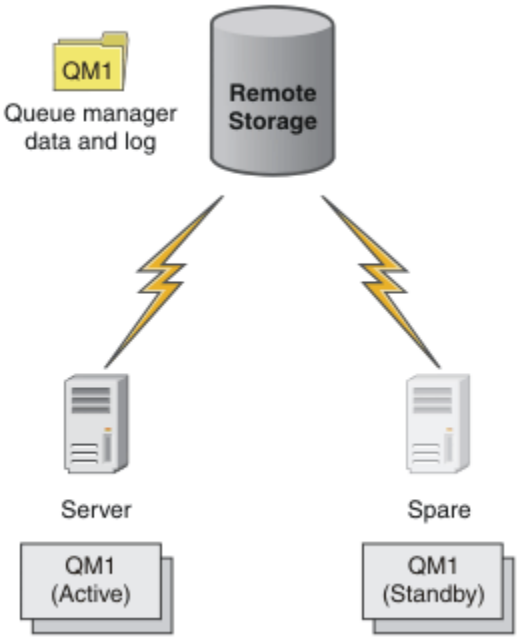
Tento obslužný program zobrazí dialogové okno s úplnými podrobnostmi o nastavení podpory MSCS produktu IBM MQ , jako je například výzva k volání podpory produktu IBM . K dispozici je volba pro uložení podrobností do souboru.

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 instance v pohotovostním režimu. Dojde-li k selhání aktivní instance, správce front s více instancemi se automaticky restartuje na záložním serveru.

Příklad konfigurace správce front s více instancemi

Obrázek 75 na stránce 458 uvádí příklad konfigurace s více instancemi pro správce front QM1. Produkt IBM MQ je nainstalován na dvou serverech, z nichž jeden je volný. Byl vytvořen jeden správce front QM1. Jedna instance QM1 je aktivní a je spuštěna na jednom serveru. Druhá instance serveru QM1 je spuštěna v pohotovostním režimu na druhém serveru, neprovádí žádné aktivní zpracování, ale je připravena převzít z aktivní instance QM1, pokud se aktivní instance nezdaří.



Obrázek 75. Správce front s více instancemi

Zamýšlíte-li používat správce front jako správce front s více instancemi, vytvořte jednoho správce front na jednom ze serverů pomocí příkazu **crtmqm** , který umístí data správce front a protokoly do sdílené síťové paměti. Na jiném serveru, než znovu vytvořit správce front, použijte příkaz **addmqinf** k vytvoření odkazu na data správce front a protokoly v síťovém úložišti.

Nyní můžete správce front spustit z jednoho ze serverů. Každý ze serverů odkazuje na stejná data a protokoly správce front; existuje pouze jeden správce front a v daném okamžiku je aktivní pouze na jednom serveru.

Správce front může být spuštěn buď jako správce front s jednou instancí, nebo jako správce front s více instancemi. V obou případech je spuštěna pouze jedna instance správce front, zpracování požadavků. Rozdíl je v tom, že při spuštění jako správce front s více instancemi se server, na kterém není spuštěna aktivní instance správce front, spustí jako instance v pohotovostním režimu, je připraven převzít z aktivní instance automaticky, pokud selže aktivní server.

Jediný ovládací prvek, který je nad kterými instancí se stane aktivní, je pořadí, ve kterém spustíte správce front na obou serverech. První instance, která získá zámky pro čtení a zápis do dat správce front, se stane aktivní instancí.

Aktivní instanci můžete odložit na jiný server, jakmile se spustí, tím, že zastavíte aktivní instanci pomocí volby přepnutí na přenos do pohotovostního režimu.

Aktivní instance QM1 má výlučný přístup k datům správce sdílených front a ke složkám protokolů, je-li spuštěn. Rezervní instance QM1 zjišťuje, kdy došlo k selhání aktivní instance, a stane se aktivní instancí. Přebírá data a protokoly QM1 ve stavu, kdy byly ponechány aktivní instancí, a přijímá nová připojení od klientů a kanálů.

Aktivní instance může selhat z různých příčin, které vedou k převzetí stavu pohotovosti:

- Selhání serveru hostujícího aktivní instanci správce front.
- Selhání konektivity mezi serverem, který je hostitelem aktivní instance správce front, a systému souborů.
- Neschopnost reagovat na procesy správce front detekovaná produktem IBM MQ, která poté ukončí práci správce front.

Informace o konfiguraci správce front můžete přidat na více serverů a vybrat libovolné dva servery, které se mají spustit jako dvojice aktivní/záložní. Existuje zde limit celkového počtu dvou instancí. Nemůžete mít dvě instance v pohotovostním režimu a jednu aktivní instanci.

Další komponenty potřebné k sestavení řešení vysoké dostupnosti

Správce front pro více instancí je jednou částí řešení vysoké dostupnosti. Chcete-li vytvořit užitečné řešení vysoké dostupnosti, potřebujete další komponenty.

- Připojení klienta a kanálu pro přenos IBM MQ připojení k počítači, který přebírá spuštění aktivní instance správce front.
- Vysoce výkonný sdílený síťový systém souborů (NFS), který spravuje zámky správně a poskytuje ochranu proti selhání média a souborového serveru.

  Důležité: Před prováděním údržby na jednotce NFS je třeba zastavit všechny instance správce front s více instancemi, které jsou spuštěny ve vašem prostředí. V případě selhání systému NFS se ujistěte, že máte zálohy konfigurace správce front, které se mají obnovit.
- Spolehlivé sítě a zdroje napájení za účelem odstranění jednotných bodů selhání v základní infrastruktuře.
- Aplikace tolerují překonání selhání. Zejména je třeba věnovat pozornost chování transakčních aplikací a aplikací, které procházejí fronty produktu IBM MQ .
- Monitorování a správa aktivních instancí a instancí v pohotovostním režimu za účelem zajištění jejich spuštění a restartování aktivních instancí, které selhaly. Ačkoli se správce front s více instancemi restartuje automaticky, musíte se ujistit, že jsou vaše instance v pohotovostním režimu spuštěny, připraveny převzít převzetí a že instance se selháním jsou znovu uvedeny do stavu online jako nové instance v pohotovostním režimu.

IBM MQ MQI clients a kanály se znovu automaticky připojí ke správci front v pohotovostním režimu, jakmile se stane aktivním. Další informace o opětovném připojení a další komponenty v řešení vysoké dostupnosti najdete v souvisejících tématech. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

podporované platformy

Správce front s více instancemi můžete vytvořit na libovolné platformě jiné nežz/OS podporované produktem IBM WebSphere MQ 7.0.1 a novějších.

Automatické opětovné připojení klienta je podporováno pro klienty MQI produktem IBM WebSphere MQ 7.0.1 a novějším.

Vytvoření správce front s více instancemi

Vytvoření správce front s více instancemi, vytvoření správce front na jednom serveru a konfigurace produktu IBM MQ na jiném serveru. Správci front s více instancemi sdílejí data a protokoly správce front.

Většina úsilí zapojování do vytváření správce front s více instancemi je úlohou nastavení dat správce sdílené fronty a souborů protokolu. Musíte vytvořit sdílené adresáře v síťovém úložišti a zpřístupnit adresáře pro jiné servery pomocí sdílených síťových sdílených složek. Tyto úlohy je třeba provést někým, kdo má administrativní oprávnění, jako je *root* na systémech UNIX and Linux . Kroky jsou následující:

1. Vytvořte sdílené prostředky pro data a soubory protokolu.
2. Vytvořte správce front na jednom serveru.
3. Spuštěním příkazu **dspmqinf** na prvním serveru shromážděte konfigurační data správce front a zkopírujte je do schránky.
4. Spusťte příkaz **addmqinf** s zkopírovanými daty za účelem vytvoření konfigurace správce front na druhém serveru.

Nespustíte příkaz **crtmqm** k opětovnému vytvoření správce front na druhém serveru.

Řízení přístupu k souboru

Je třeba dbát na to, aby uživatel a skupina `mqm` na všech ostatních serverech měly oprávnění pro přístup ke sdílením.

V systému UNIX and Linuxmusíte ve všech systémech učinit `uid` a `gid` produktu `mqm` stejné. Možná budete muset upravit `/etc/passwd` na každém systému, abyste nastavili obecné `uid` a `gid` pro `mqm`, a pak znovu zaveďte systém.

V systému Microsoft Windowsmusí mít ID uživatele, který spouští procesy správce front, úplné oprávnění pro řízení k adresářům obsahujícím data správce front a soubory protokolu. Oprávnění můžete nakonfigurovat dvěma způsoby:

1. Vytvořte správce front s globální skupinou jako alternativního činitele zabezpečení. Autorizujte globální skupinu, aby měla úplný přístup pro řízení k adresářům obsahujícím data správce front a soubory protokolu, viz “Zabezpečení dat správce sdílených front a adresářů protokolů a souborů v systému Windows” na stránce 487. Vytvořte ID uživatele, pod kterým je spuštěn správce front, člena globální skupiny. Lokální uživatele nelze vytvořit jako člena globální skupiny, takže procesy správce front musí být spuštěny pod ID uživatele domény. ID uživatele domény musí být členem lokální skupiny `mqm`. Úloha “Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462demonstruje, jak nastavit správce front s více instancemi pomocí souborů zabezpečených tímto způsobem.
2. Vytvořte správce front v řadiči domény tak, aby lokální skupina `mqm` měla rozsah domény, "lokální doména". Zabezpečte sdílení souboru s lokálním serverem `mqm`a spusťte procesy správce front ve všech instancích správce front v rámci stejné lokální skupiny produktu `mqm` . Úloha “Vytvoření správce front s více instancemi na řadičích domény Windows” na stránce 477demonstruje, jak nastavit správce front s více instancemi pomocí souborů zabezpečených tímto způsobem.

Informace o konfiguraci

Nakonfigurujte tolik instancí správce front, kolik potřebujete, úpravou informací o konfiguraci správce front produktu IBM MQ na každém serveru. Každý server musí mít nainstalovánu stejnou verzi produktu IBM MQ na kompatibilní úrovni oprav. Příkazy, **dspmqinf** a **addmqinf** vám pomáhají konfigurovat další instance správce front. Alternativně můžete soubory `mqs.ini` a `qm.ini` upravit přímo. Témata, “Vytvoření správce front s více instancemi v systému Linux” na stránce 499, “Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462a “Vytvoření správce front s více instancemi na řadičích domény Windows” na stránce 477 představují příklady konfigurace správce front s více instancemi.

V systémech Windows, UNIX and Linux můžete sdílet jeden soubor `mqs.ini` tak, že jej umístíte na sdílenou síťovou stránku a nastavíte proměnnou prostředí **AMQ_MQS_INI_LOCATION** tak, aby ukazovala na jeho hodnotu.

Omezení

1. Konfigurovat více instancí stejného správce front pouze na serverech se stejným operačním systémem, architekturou a endiannerem. Oba stroje musí být například buď 32bitové, nebo 64bitové.
2. Všechny instalace produktu IBM MQ musí být na úrovni verze 7.0.1 nebo vyšší.
3. Typicky jsou aktivní a záložní instalace udržovány na stejné úrovni údržby. Chcete-li zkontrolovat, zda je třeba provést upgrade všech instalací, prostudujte si pokyny k údržbě pro každý přechod na vyšší verzi.

   Všimněte si, že úrovně údržby aktivních a pasivních správců front musí být identické.
4. Sdílejte data správce front a protokoly pouze mezi správci front, kteří jsou konfigurováni se stejným uživatelem produktu IBM MQ , skupinou a mechanismem řízení přístupu. IBM i Například sdílení sítě nastavené na serveru Linux může obsahovat samostatná data správce front a protokoly pro správce front produktu UNIX and Linux , ale nemůže obsahovat data správce front, která byla použita produktem IBM i.

   IBM i Můžete vytvořit více sdílených prostředků ve stejném síťovém úložném prostoru pro IBM i a pro systémy UNIX , pokud se sdílení liší. Odlišné vlastníky můžete dát různým vlastníkům. Omezení je důsledkem různých názvů používaných pro uživatele a skupiny produktu IBM MQ mezi produkty UNIX a IBM i. Skutečnost, že uživatel a skupina mohou mít stejné `uid` a `gid` , nezklidňuje omezení.

5. V systémech UNIX and Linux nakonfigurujte sdílený systém souborů v síťovém úložišti pomocí volby `hard`, přerušitelný, místo připojení `soft` . Pevné přerušitelné připojení vynutí, aby správce front uvázl, dokud nebude přerušen systémovým voláním. Měkká připojení nezaručujte konzistenci dat po selhání serveru.
6. Sdílený protokol a datové adresáře nemohou být uloženy v systému souborů FAT nebo v systému souborů NFSv3 . Pro správce front s více instancemi v systému Windowsmusí být k síťovému úložišti přistupovat prostřednictvím protokolu CIFS (Common Internet File System) používaného sítěmi Windows .
7. z/OS Produkt z/OS nepodporuje správce front s více instancemi. Použít skupiny sdílení front.

   Znovu připojitelné klienty pracují se správci front produktu z/OS .

Windows *Windows domén a správců front s více instancemi*

Správce front s více instancemi v produktu Windows vyžaduje, aby byla sdílena data a protokoly. Sdílení musí být přístupné pro všechny instance správce front spuštěných na různých serverech nebo pracovních stanicích. Konfigurujte správce front a sdílejte jej jako součást domény produktu Windows . Správce front může být spuštěn na pracovní stanici nebo na serveru domén nebo na řadiči domény.

Před konfigurací správce front s více instancemi si přečtěte téma “Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows” na stránce 490 a “Zabezpečení dat správce sdílených front a adresářů protokolů a souborů v systému Windows” na stránce 487 a zkontrolujte, jak řídit přístup k datům správce front a protokolových souborů. Témata jsou vzdělávací; chcete-li přejít přímo k nastavení sdílených adresářů pro správce front s více instancemi v doméně Windows , viz “Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462.

Spustit správce front s více instancemi na pracovních stanicích nebo na serverech domény

V produktu IBM WebSphere MQ 7.1jsou správci front s více instancemi spouštěny na pracovní stanici nebo na serveru, který je členem domény. Chcete-li spustit správce front s více instancemi v produktu Windows, je třeba mít k dispozici řadič domény, souborový server a dvě pracovní stanice nebo servery provozující stejného správce front připojeného ke stejné doméně.

Změna, která umožňuje spustit správce front s více instancemi na libovolném serveru nebo pracovní stanici v doméně, je to, že můžete nyní vytvořit správce front s další skupinou zabezpečení. Další skupina zabezpečení je předána v příkazu **`crtmqm`** , v parametru `-a` . Zabezpečte adresáře, které obsahují data správce front, a protokoly se skupinou. ID uživatele, který spouští procesy správce front, musí být členem této skupiny. Když správce front přistupuje k adresářům, produkt Windows zkontroluje oprávnění, která má ID uživatele pro přístup k adresářům. Uvede-li skupina i rozsah domény ID uživatele, bude mít ID uživatele, který spouští procesy správce front, pověření z globální skupiny. Je-li správce front spuštěn na jiném serveru, může mít ID uživatele, který spouští procesy správce front, stejná pověření. ID uživatele nemusí být stejné. Musí být členem alternativní skupiny zabezpečení, stejně jako člen lokální skupiny `mqm` .

Podrobnosti o vytvoření správce front s více instancemi viz “Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462 .

Pro konfiguraci domény a pro servery a pracovní stanice domény je třeba provést více kroků. Je třeba pochopit, jak produkt Windows autorizuje přístup správce front k jeho datům a adresářům protokolů. Pokud si nejste jisti, jak jsou procesy správce front autorizovány pro přístup k protokolové a datové soubory, přečtěte si téma “Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows” na stránce 490. Toto téma obsahuje dvě úlohy, které vám pomohou porozumět krokům, které je třeba provést. Úlohy jsou “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 492 a “Čtení a zápis dat a souborů protokolu autorizovaných alternativní lokální skupinou zabezpečení” na stránce 495. Další téma, “Zabezpečení dat správce sdílených front a adresářů protokolů a souborů v systému Windows” na stránce 487, vysvětluje, jak zabezpečit sdílené adresáře obsahující data správce front a soubory protokolu s alternativní skupinou zabezpečení. Toto

téma obsahuje čtyři úlohy pro nastavení domény produktu Windows , vytvoření sdílení souboru, instalaci produktu IBM MQ for Windowsa konfigurování správce front pro použití sdílení. Úlohy jsou následující:

1. “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465.
2. “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 469.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows” na stránce 471.
4. “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 474.

Potom můžete provést úlohu “Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462pomocí domény. Tyto úlohy slouží k prozkoumání nastavení správce front pro více instancí před přenosem vašich znalostí do produkční domény.

Spustit správce front s více instancemi na řadičích domény

Data správce front by mohla být zabezpečena pomocí skupiny domén `mqm` . Jak se vysvětluje téma “Zabezpečení dat správce sdílených front a adresářů protokolů a souborů v systému Windows” na stránce 487 , nemůžete sdílet adresáře zabezpečené s lokální skupinou `mqm` na pracovních stanicích nebo serverech. Avšak na řadičích domény všechny skupiny a řídicí služby mají rozsah domény. Pokud instalujete produkt IBM MQ for Windows na řadič domény, data správce front a soubory protokolu jsou zabezpečeny skupinou `mqm` domény, kterou lze sdílet. Postupujte podle kroků uvedených v úloze “Vytvoření správce front s více instancemi na řadičích domény Windows” na stránce 477 a nakonfigurujte správce front s více instancemi na řadičích domény.

Související informace

Správa autorizace a řízení přístupu

Jak používat uzly klastru serveru Windows jako řadiče domény

Windows *Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows*

Příklad ukazuje, jak nastavit správce front s více instancemi na systému Windows na pracovní stanici nebo na serveru, který je součástí domény Windows . Server nemusí být řadič domény. Nastavení demonstruje zahrnuté koncepce, spíše než aby bylo produkční měřítko. Tento příklad je založen na serveru Windows Server 2008. Tyto kroky se mohou lišit od dalších verzí serveru Windows .

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
: Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
: Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
: Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

V systému Windowsnení nutné ověřovat systém souborů, do kterého chcete ukládat data správce front a soubory žurnálu. Procedura kontroly, Ověření chování sdíleného systému souborů, je použitelná pro UNIX and Linux. V systému Windowsjsou kontroly vždy úspěšné.

Postupujte podle kroků uvedených v následujících úlohách. Úlohy vytvoří řadič domény a doménu, nainstalujte produkt IBM MQ for Windows na jeden server a vytvořte sdílení souboru pro data a soubory protokolu. Pokud konfigurujete existující řadič domény, můžete zjistit, že je užitečné vyzkoušet si kroky na novém serveru Windows Server 2008. Kroky je možné upravit podle své domény.

1. “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465.
2. “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 469.
3. “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows” na stránce 471.
4. “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 474.

Informace o této úloze

Tato úloha je jednou z posloupností úloh pro konfiguraci řadiče domény a dvou serverů v doméně za účelem spouštění instancí správce front. V této úloze nakonfigurujete druhý server, produkt *venus*, aby spustil jinou instanci správce front *QMGR*. Postupujte podle kroků uvedených v této úloze a vytvořte druhou instanci správce front, *QMGR*a otestujte, zda pracuje.

Tato úloha je oddělena od čtyř úloh v předchozí sekci. Obsahuje kroky, které převádějí jednoho správce front instance na správce front s více instancemi. Všechny ostatní kroky jsou společné pro jednotlivé správce front nebo správce front s více instancemi.

Postup

1. Nakonfigurujte druhý server ke spuštění produktu IBM MQ for Windows.
   a) Chcete-li vytvořit druhý server domény, proveďte kroky v úloze “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 469 . V této posloupnosti úloh se druhý server nazývá *venus*.

      Tip: Vytvořte druhou instalaci s použitím stejných výchozích nastavení instalace pro produkt IBM MQ na každém ze dvou serverů. Pokud se výchozí hodnoty liší, možná budete muset upravit proměnné `Předpona` a `InstallationName` ve stanze *QMGR* **`QueueManager`** v konfiguračním souboru IBM MQ `mqs.ini`. Proměnné odkazují na cesty, které se mohou lišit pro každou instalaci a správce front na každém serveru. Pokud cesty zůstávají stejné na každém serveru, je jednodušší konfigurovat správce front s více instancemi.
2. Vytvořte druhou instanci produktu *QMGR* v systému *venus*.
   a) Pokud *QMGR* v systému *mars* neexistuje, proveďte úlohu “Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 474a vytvořte ji.
   b) Zkontrolujte hodnoty parametrů `Předpona` a `InstallationName` , které jsou správné pro produkt *venus*.

      V systému *mars*spusťte příkaz **`dspmqinf`** :

      ```
      dspmqinf QMGR
      ```

      Odezva systému:

      ```
      QueueManager:
      Name=QMGR
      Directory=QMGR
      Prefix=C:\ProgramData\IBM\MQ
      DataPath=\\sun\wmq\data\QMGR
      InstallationName=Installation1
      ```
   c) Okopírujte strojově čitelnou formu stanzy **`QueueManager`** do schránky.

V systému *mars* spusťte příkaz **dspmqinf** znovu s parametrem `-o command` .

```
dspmqinf -o command QMGR
```

Odezva systému:

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

d) V systému *venus* spusťte příkaz **addmqinf** ze schránky a vytvořte instanci správce front v systému *venus*.

V případě potřeby upravte příkaz tak, aby vyhovoval rozdílům v parametrech `Předpona` nebo `InstallationName` .

```
addmqinf -s QueueManager -v Name=QMGR
-v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
-v DataPath=\\sun\wmq\data\QMGR
```

```
IBM MQ configuration information added.
```

3. Spusťte správce front *QMGR* v systému *venus*a povolit instance v pohotovostním režimu.

a) Kontrola *QMGR* na *mars* je zastavena.

V systému *mars*spusťte příkaz **dspmq** :

```
dspmq -m QMGR
```

Odezva systému závisí na tom, jak byl správce front zastaven; například:

```
C:\Users\Administrator>dspmq -m QMGR
QMNAME(QMGR) STATUS(Ended immediately)
```

b) V systému *venus* spusťte příkaz **strmqm** ke spuštění příkazu *QMGR* , který povoluje standbys:

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

Výsledky

Chcete-li otestovat přepínače správce front s více instancemi, proveďte následující kroky:

1. V systému *mars*spusťte příkaz **strmqm** , který spustí příkaz *QMGR* povolující standbys:

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
A standby instance of queue manager 'QMGR' has been started.
The active instance is running elsewhere.
```

2. V systému *venus* spusťte příkaz **endmqm** :

```
endmqm -r -s -i QMGR
```

Odezva systému na *venus*:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended, permitting switchover to
a standby instance.
```

A v systému *mars*:

```
dspmq
QMNAME(QMGR) STATUS(Running as standby)
C:\Users\wmquser2>dspmq
QMNAME(QMGR) STATUS(Running as standby)
C:\Users\wmquser2>dspmq
QMNAME(QMGR)  STATUS(Running)
```

Jak pokračovat dále

Chcete-li ověřit správce front s více instancemi pomocí ukázkových programů, přečtěte si téma “Ověření správce front s více instancemi v systému Windows” na stránce 485.

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*. Nakonfiguruje globální skupinu Domain mqm v doméně, se správnými právy a s jedním uživatelem.

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
: Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
: Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
: Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Kroky úlohy jsou konzistentní s produktem Windows Server 2008, který je nainstalován, ale není nakonfigurován s žádnou rolí. Pokud konfigurujete existující řadič domény, můžete zjistit, že je užitečné vyzkoušet si kroky na novém serveru Windows Server 2008. Kroky je možné upravit podle své domény.

Informace o této úloze

V této úloze vytvoříte Active Directory a doménu DNS na novém řadiči domény. Poté ji nakonfigurujete tak, aby byl připraven k instalaci produktu IBM MQ na jiných serverech a pracovních stanicích, které se připojí k doméně. Pokud nejste obeznámeni s instalací a konfigurací adresáře Active Directory pro vytvoření domény produktu Windows , postupujte podle této úlohy. Chcete-li vytvořit konfiguraci správce front s více instancemi, je třeba vytvořit doménu produktu Windows . Úloha není určena k tomu, aby vás nejlépe vedla ke konfiguraci domény produktu Windows . Chcete-li implementovat správce front s více instancemi v produkčním prostředí, musíte se seznámit s dokumentací produktu Windows .

Během úlohy proveďte následující kroky:

1. Nainstalujte Active Directory.
2. Přidejte doménu.
3. Přidejte doménu do DNS.
4. Vytvořte globální skupinu `Domain mqm` a udělte mu správná práva.
5. Přidejte uživatele a vytvořte jej jako člena globální skupiny `Domain mqm`.

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu "Windows domén a správců front s více instancemi" na stránce 461.

Pro účely úlohy je název hostitele řadiče domény *sun*a tyto dva servery IBM MQ se nazývají *mars* a *venus*. Doména se nazývá *wmq.example.com*. Všechny kurzívy v úloze můžete nahradit názvy dle vlastního výběru.

Postup

1. Přihlaste se k řadiči domény *sun*jako administrátor lokálního systému nebo administrátor produktu `Workgroup` .

   Je-li server již konfigurován jako řadič domény, musíte se přihlásit jako administrátor domény.
2. Spusťte průvodce Active Directory Domain Services.

   a) Klepněte na nabídku **Start** > **Spustit ...** Zadejte `dcpromo` a klepněte na **OK**.

   Nejsou-li binární soubory Active Directory již nainstalovány, produkt Windows nainstaluje soubory automaticky.
3. V prvním okně průvodce ponechte zaškrtávací políčko **Použít rozšířenou instalaci režimu** prázdné. Klepněte na tlačítko **Další** > **Další** a klepněte na volbu **Vytvořit novou doménu v novém lese** > **Další**.
4. Zadejte *wmq.example.com* do pole **FQDN kořenové domény lesa** . Klepněte na tlačítko **Další**.
5. V okně Nastavit funkční úroveň doménové struktury vyberte volbu **Windows Server 2003**nebo novější ze seznamu **Funkční úrovně doménové struktury** > **Další**.

   Nejstarší úroveň serveru Windows , která je podporována produktem IBM MQ , je Windows Server 2003.
6. Volitelné: V okně Nastavit funkční úroveň domény vyberte volbu **Windows Server 2003**nebo novější ze seznamu **Funkční úrovně domény** > **Další**.

   Tento krok je nezbytný pouze v případě, že nastavíte funkční úroveň doménové struktury na **Windows Server 2003**.
7. Otevře se okno Další volby řadiče domény s volbou **Server DNS** jako přídavnou volbou. Klepněte na tlačítko **Další** a **Ano** , chcete-li vymazat okno s varováním.

Tip: Je-li již server DNS nainstalován, tato volba se vám nepředkládá. Pokud chcete tuto úlohu sledovat přesně, odeberte všechny role z tohoto řadiče domény a začněte znovu.

8. Ponechejte adresáře `Database`, `Log Filesa` SYSVOL nezměněných; klepněte na tlačítko **Další**.
9. Do polí **Heslo** a **Potvrdit heslo** zadejte heslo do pole Heslo administrátora režimu obnovy adresářových služeb. Klepněte na tlačítko **Další** > **Další**. V závěrečném okně průvodce vyberte volbu **Znovu spustit po dokončení** .
10. Když se řadič domény restartuje, přihlaste se jako *wmq*\`Adminstrator`.

    Správce serveru se spustí automaticky.
11. Otevřete složku *wmq.example.com*\`Users` .
    a) Otevřete produkt **Server Manager** > **Role** > **Active Directory Domain Services** > ***wmq.example.com*** > **Users**.
12. Klepněte pravým tlačítkem myši na nabídku **Uživatelé** > **Nová** > **Skupina**.
    a) Do pole **Název skupiny** zadejte název skupiny.

    Poznámka: Upřednostňovaný název skupiny je `Domain mqm`. Zadejte jej přesně tak, jak je uveden.

    - Nazváním skupiny `Domain mqm` se upraví chování "Průvodce přípravou produktu IBM MQ" na pracovní stanici nebo serveru domény. Způsobí to, že "Průvodce přípravou produktu IBM MQ" automaticky přidá skupinu `Domain mqm` do lokální skupiny `mqm` v každé nové instalaci produktu IBM MQ v dané doméně.
    - Pracovní stanice nebo servery můžete instalovat i v doméně bez globální skupiny `Domain mqm`. Pokud tak učiníte, musíte definovat skupinu se stejnými vlastnostmi 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 skupině** a **Povolit Číst groupMembershipSAM** , která se bude používat pro globální skupinu `Domain mqm` .
    a) V řádku s akcemi správce serveru klepněte na volbu **Pohled** > **Rozšířené vlastnosti**.
    b) Ve stromu navigace správce serveru klepněte na volbu **Uživatelé** .
    c) V okně Users klepněte pravým tlačítkem myši na položku **Domain mqm** > **Vlastnosti** .
    d) Klepněte na volbu **Zabezpečení** > **Rozšířené** > **Přidat ...**. Zadejte `Domain mqm` a klepněte na **Zkontrolovat jména** > **OK**.

    Pole **Název** je předem vyplněno řetězcem `Domain mqm (`*domain name*`\Domain mqm)`.
    e) Klepněte na příkaz **Vlastnosti**. V seznamu **Použít na** vyberte položku **Podřízené objekty uživatele**.
    f) V seznamu **Oprávnění** vyberte zaškrtávací políčka **Číst členství ve skupině** a **Číst groupMembershipSAM Povolit** . Klepněte na tlačítko **OK** > **Použít** > **OK** > **OK**.
14. Přidejte dva nebo více uživatelů do globální skupiny `Domain mqm` .

    Jeden uživatel, *wmquser1* v tomto příkladu, spouští službu IBM MQ a druhý uživatel, *wmquser2* , se používá interaktivně.

Pro vytvoření správce front, který používá alternativní skupinu zabezpečení v konfiguraci domény, je vyžadován uživatel domény. Nestačí, aby ID uživatele bylo administrátorem, ačkoli má administrátor oprávnění ke spuštění příkazu **crtmqm** . Uživatel domény, který může být administrátor, musí být členem lokální skupiny `mqm` a také alternativní skupiny zabezpečení.

V tomto příkladu vytvoříte *wmquser1* a *wmquser2* členy globální skupiny `Domain mqm` . Průvodce "Příprava produktu IBM MQ " automaticky nakonfiguruje `Domain mqm` jako člena lokální skupiny `mqm` , kde se průvodce spustí.

Chcete-li spustit službu IBM MQ pro každou instalaci produktu IBM MQ na jednom počítači, musíte zadat jiného uživatele. Stejné uživatele můžete znovu použít na různých počítačích.

a) Ve stromu navigace správce serveru klepněte na nabídku **Uživatelé** > **Nový** > **Uživatel** .

b) V okně Nový objekt-Uživatel zadejte *wmquser1* do pole **Přihlašovací jméno uživatele** . Do pole **Křestní jméno** zadejte *WebSphere* a do pole **Příjmení** zadejte *MQ1* . Klepněte na tlačítko **Další**.

c) Zadejte heslo do polí **Heslo** a **Potvrdit heslo** a zrušte označení zaškrtávacího políčka **Uživatel musí změnit heslo při příštím přihlášení** . Klepněte na tlačítko **Další** > **Dokončit**.

d) V okně Users klepněte pravým tlačítkem myši na ***WebSphere MQ*** > **Přidat do skupiny ...**. Zadejte `Domain mqm` a klepněte na **Zkontrolovat názvy** > **OK** > **OK**.

e) Opakujte kroky a až d , chcete-li přidat *WebSphere MQ2* jako *wmquser2* .

15. Spuštění IBM MQ jako služby.

Pokud potřebujete spustit produkt IBM MQ jako službu a poté poskytnout uživateli domény (který jste získali od administrátora domény) přístup ke službě jako službu, proveďte následující postup:

a) Klepněte na tlačítko **Start > Spustit ...**.

Zadejte příkaz `secpol.msc` a klepněte na tlačítko **OK**.

b) Otevřete **Nastavení zabezpečení > Lokální zásady > Přiřazení uživatelských práv**.

V seznamu zásad klepněte pravým tlačítkem myši na **Přihlásit se jako služba > Vlastnosti**.

c) Klepněte na volbu **Přidat uživatele nebo skupinu ...**

Zadejte jméno uživatele, kterého jste získali od administrátora domény, a klepněte na **Kontrolovat názvy** .

d) Budete-li vyzváni oknem Zabezpečení produktu Windows , zadejte jméno uživatele a heslo účtu uživatele nebo administrátora účtu s dostatečným oprávněním a klepněte na tlačítko **OK > Použít > OK**.

Zavřete okno Lokální zásada zabezpečení.

Poznámka: Na serveru Windows Server 2008 a Windows Server 2012 je funkce UAC (User Account Control) povolena standardně.

Funkce UAC omezuje akce, které mohou uživatelé provádět na určitých zařízeních operačního systému, i když jsou členy skupiny Administrátoři. Musíte provést příslušné kroky, abyste tato omezení překonali.

Jak pokračovat dále

Pokračujte k další úloze “Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows” na stránce 469.

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, které jsou autorizovány 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 škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li vytvořit řadič domény, *sun*pro doménu *wmq.example.com*, proveďte kroky v části “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465 . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
2. Informace o dalších verzích produktu Windows , na kterých lze spustit produkt IBM MQ , najdete v tématu Hardwarové a softwarové požadavky na systémech Windows .

Informace o této úloze

V této úloze nakonfigurujete server Windows Server 2008 s názvem *mars*jako člen domény *wmq.example.com* . Nainstalujte produkt IBM MQa nakonfigurujte instalaci tak, aby se spouštěla jako člen domény *wmq.example.com* .

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 461.

Pro účely úlohy je název hostitele řadiče domény *sun*a tyto dva servery IBM MQ se nazývají *mars* a *venus*. Doména se nazývá *wmq.example.com*. Všechny kurzívy v úloze můžete nahradit názvy dle vlastního výběru.

Postup

1. Přidejte řadič domény, *sun.wmq.example.com* do *mars* jako server DNS.
   a) V produktu *mars*se přihlaste jako *mars*\Administrator a klepněte na tlačítko **Spustit**.
   b) Klepněte pravým tlačítkem myši na **Síť** > **Vlastnosti** > **Spravovat síťová připojení**.
   c) Klepněte pravým tlačítkem myši na síťový adaptér a poté klepněte na volbu **Vlastnosti**.

      Systém odpoví v okně Vlastnosti připojení k místní síti, které uvádí položky, které připojení používá.
   d) Ze seznamu položek v okně Vlastnosti připojení lokální oblasti vyberte ze seznamu položek **Internet Protocol verze 4** nebo **Internet Protocol verze 6** . Klepněte na volbu **Vlastnosti** > **Rozšířené ...** a klepněte na kartu **DNS** .
   e) Pod adresou serveru DNS klepněte na **Přidat ...**.
   f) Zadejte adresu IP řadiče domény, který je také serverem DNS, a klepněte na tlačítko **Přidat**.

g) Klepněte na volbu **Připojit tyto přípony systému DNS** > **Přidat ...**.

h) Zadejte *wmq.example.com* a klepněte na **Přidat**.

i) Zadejte *wmq.example.com* do pole **Přípona systému DNS pro toto připojení** .

j) Vyberte volbu **Registrovat tuto adresu připojení v DNS** a **Použít příponu tohoto připojení v registraci DNS**. Klepněte na tlačítko **OK** > **OK** > **Zavřít** .

k) Otevřete příkazové okno a zadejte příkaz **ipconfig /all** , abyste zkontrolli nastavení TCP/IP.

2. V systému *mars*přidejte počítač do domény *wmq.example.com* .

a) Klepněte na tlačítko **Spustit**

b) Klepněte pravým tlačítkem myši na **Počítač** > **Vlastnosti**. V části Název počítače, domény a nastavení pracovní skupiny klepněte na volbu **Změnit nastavení**.

c) V oknech vlastností systému klepněte na tlačítko **Změnit ...**.

d) Klepněte na doménu, zadejte *wmq.example.com*a klepněte na **OK**.

e) Zadejte **Jméno uživatele** a **Heslo** administrátora řadiče domény, který má oprávnění k povolení k připojení počítače k doméně, a klepněte na tlačítko **OK**.

f) Klepněte na tlačítko **OK** > **OK** > **Zavřít** > **Restartovat nyní** v odpovědi na zprávu "Vítejte v doméně *wmq.example.com*" .

3. Zkontrolujte, zda je počítač členem domény *wmq.example.com*

a) V systému *sun*se přihlaste k řadiči domény jako *wmq*\Administrator.

b) Otevřete produkt **Server Manager** > **Active Directory Domain Services** > ***wmq.example.com*** > **Počítače** a zkontrolujte, zda je v okně Počítače správně uveden *mars* .

4. Nainstalujte IBM MQ for Windows na *mars*.

Další informace o spuštění průvodce instalací produktu IBM MQ for Windows naleznete v tématu Instalace serveru IBM MQ v systému Windows .

a) V systému *mars*se přihlaste jako lokální administrátor, *mars*\Administrator.

b) Spusťte příkaz **Setup** na instalačním médiu produktu IBM MQ for Windows .

Spustí se příruční panel produktu IBM MQ .

c) Klepněte na **Softwarové požadavky** , chcete-li zkontrolovat, zda je nainstalován předem vyžadovaný software.

d) Klepněte na **Konfigurace sítě** > **Ano** , chcete-li konfigurovat ID uživatele domény.

Úloha, “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465, konfiguruje ID uživatele domény pro tuto sadu úloh.

e) Klepněte na volbu **IBM MQ Instalace**, vyberte jazyk instalace a klepněte na volbu Spustit instalační program produktu IBM MQ .

f) Potvrďte licenční smlouvu a klepněte na tlačítko **Další** > **Další** > **Instalovat** , chcete-li přijmout výchozí konfiguraci. Čekejte, až se instalace dokončí, a klepněte na tlačítko **Dokončit**.

Možná budete chtít změnit název instalace, instalovat různé komponenty, konfigurovat jiný adresář pro data správce front a protokoly nebo instalovat do jiného adresáře. Pokud ano, klepněte na volbu **Vlastní** namísto volby **Typická**.

Produkt IBM MQ je instalován a instalační program spustí průvodce "Příprava produktu IBM MQ " .

Důležité: Ještě nespouštějte průvodce.

5. Nakonfigurujte uživatele, který bude spouštět službu IBM MQ se správnou volbou **Spustit jako služba** .

Vyberte, zda chcete konfigurovat lokální skupinu mqm , skupinu Domain mqm nebo uživatele, který bude spouštět službu IBM MQ se správnou hodnotou. V tomto příkladu dáte uživateli právo.

a) Klepněte na nabídku **Start** > **Spustit ...**, Zadejte příkaz **secpol.msc** a klepněte na **OK**.

b) Otevřete **Nastavení zabezpečení** > **Lokální zásady** > **Přiřazení uživatelských práv**. V seznamu zásad klepněte pravým tlačítkem myši na **Přihlásit se jako služba** > **Vlastnosti** .

c) Klepněte na volbu **Přidat uživatele nebo skupinu ...** a zadejte *wmquser1* a klepněte na **Kontrolovat názvy**

d) Zadejte jméno uživatele a heslo administrátora domény, *wmq*\Administratora klepněte na tlačítko **OK** > **Použít** > **OK**. Zavřete okno Lokální zásada zabezpečení.

6. Spusťte průvodce "Příprava produktu IBM MQ " .

   Další informace o spuštění průvodce "Příprava produktu IBM MQ " naleznete v tématu Konfigurace prostoru IBM MQ pomocí Průvodce přípravou produktu IBM MQ.

   a) Instalačnímu programu IBM MQ se automaticky spustí "Příprava produktu IBM MQ " .

      Chcete-li průvodce spustit ručně, najděte zástupce složky "Prepare IBM MQ " ve složce **Start** > **Všechny programy** > **IBM MQ** . Vyberte zástupce, který odpovídá instalaci produktu IBM MQ v konfiguraci s více instalačními programy.

   b) Klepněte na tlačítko **Další** a v odpovědi na otázku "Označit, zda existuje řadič domény Windows 2000 nebo novější v síti", klepněte na tlačítko **Ano** .

   c) Klepněte na tlačítko **Ano** > **Další** v okně první konfigurace produktu IBM MQ for Windows pro uživatele domény produktu Windows .

   d) V druhém okně Konfigurace IBM MQ for Windows pro uživatele domény Windows zadejte *wmq* do pole **Doména** . Zadejte *wmquser1* do pole **Jméno uživatele** a heslo, pokud jste jej nastavili, v poli **Heslo** . Klepněte na tlačítko **Další**.

      Průvodce konfiguruje a spouští produkt IBM MQ s parametrem *wmquser1*.

   e) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí zaškrtávacích políček podle potřeby a klepněte na tlačítko **Dokončit**.

Jak pokračovat dále

1. Proveďte úlohu “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 492, abyste ověřili, že instalace a konfigurace fungují správně.
2. Proveďte úlohu “Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows” na stránce 471, chcete-li konfigurovat sdílení souborů pro ukládání 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, které jsou autorizovány 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 škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li provést tuto úlohu přesně podle popisu, proveďte kroky v úloze "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 465, chcete-li vytvořit doménu *sun.wmq.example.com* na řadiči domény *sun*. Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.

Informace o této úloze

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu "Windows domén a správců front s více instancemi" na stránce 461.

V rámci úlohy vytvoříte sdílení obsahující data a adresář protokolu a globální skupinu pro autorizaci přístupu ke sdílení. Předáte název globální skupiny, která autorizuje podíl na příkazu **crtmqm** ve svém parametru -a . Globální skupina vám poskytuje flexibilitu oddělování uživatelů tohoto sdílení od uživatelů jiných sdílených prostředků. Nepotřebujete-li tuto flexibilitu, autorizujte ji raději se skupinou Domain mqm , než vytvoříte novou globální skupinu.

Globální skupina použitá pro sdílení v této úloze se nazývá *wmqha*, a sdílení se nazývá *wmq*. Jsou definovány na řadiči domény *sun* v doméně Windows *wmq.example.com*. Podíl má úplná oprávnění k řízení pro globální skupinu *wmqha*. Zaměňte názvy kurzívou v úloze s názvy dle vašeho výběru.

Pro účely této úlohy je řadičem domény stejný server jako souborový server. V praktických aplikacích rozdělte adresář a souborové služby mezi různými servery pro výkon a dostupnost.

Musíte nakonfigurovat ID uživatele, pod kterým je spuštěn správce front, aby byl členem dvou skupin. Musí se jednat o člena lokální skupiny mqm na serveru IBM MQ a globální skupině *wmqha* .

Je-li správce front spuštěn jako služba v této sadě úloh, je spuštěn pod ID uživatele *wmquser1*, takže *wmquser1* musí být členem *wmqha*. Je-li správce front spuštěn interaktivně, spustí se pod ID uživatele *wmquser2*, takže *wmquser2* musí být členem *wmqha*. Jak *wmquser1* , tak *wmquser2* jsou členy globální skupiny Domain mqm. Domain mqm je členem lokální skupiny mqm na serverech *mars* a *venus* IBM MQ . Proto jsou *wmquser1* a *wmquser2* členy lokální skupiny mqm na obou serverech IBM MQ .

Postup

1. Přihlaste se k řadiči domény, *sun.wmq.example.com* jako administrátor domény.
2. Vytvořte globální skupinu *wmqha*.
   a) Otevřete produkt **Server Manager** > **Role** > **Active Directory Domain Services** > ***wmq.example.com*** > **Users**.
   b) Otevřete složku *wmq.example.com*\Users .
   c) Klepněte pravým tlačítkem myši na nabídku **Uživatelé** > **Nová** > **Skupina**.
   d) Zadejte *wmqha* do pole **Název skupiny** .
   e) Ponechte **Globální** klepnuto jako **Rozsah skupiny** a **Zabezpečení** jako **Typ skupiny**. Klepněte na tlačítko **OK**.
3. Přidejte uživatele domény *wmquser1* a *wmquser2* do globální skupiny, *wmqha*.
   a) Ve stromu navigace správce serveru klepněte na volbu **Uživatelé** a klepněte pravým tlačítkem myši na položku ***wmqha*** > **Vlastnosti** v seznamu uživatelů.

b) Klepněte na kartu Členové v okně Vlastnosti *wmqha* .

c) Klepněte na tlačítko **Přidat ...** ; napište *wmquser1 ; wmquser2* a klepněte na **Zkontrolovat názvy** > **OK** > **Použít** > **OK**.

4. Vytvořte adresářový strom, který bude obsahovat data správce front a soubory protokolu.

a) Otevřete příkazový řádek.

b) Zadejte příkaz:

```
md c:\wmq\data, c:\wmq\logs
```

5. Autorizujte globální skupinu *wmqha* , aby měla oprávnění k úplnému řízení pro adresáře a sdílení produktu *c:\wmq* .

a) V produktu Windows Explorer klepněte pravým tlačítkem myši na ***c: \wmq*** > **Vlastnosti**.

b) Klepněte na kartu **Zabezpečení** a klepněte na volbu **Rozšířené** > **Upravit ...**.

c) Zrušte označení zaškrtávacího políčka **Zahrnout oprávnění k dědičné oprávnění u vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení produktu Windows .

d) Vyberte řádky pro uživatele v seznamu **Položky oprávnění** a klepněte na tlačítko **Odebrat**. Řádky pro SYSTEM, Administrators a CREATOR OWNER ponechejte v seznamu **Položky oprávnění**.

e) Klepněte na tlačítko **Přidat ...**. a zadejte název globální skupiny *wmqha*. Klepněte na volbu **Zkontrolovat názvy** > **OK**.

f) V okně Položka oprávnění pro wmq vyberte **Úplné řízení** v seznamu **Oprávnění**.

g) Klepněte na tlačítko **OK** > **Použít** > **OK** > **OK** > **OK**

h) V produktu Windows Explorer klepněte pravým tlačítkem myši na ***c: \wmq*** > **Sdílet ...**.

i) Klepněte na volbu **Rozšířené sdílení ...** a vyberte zaškrtávací políčko **Sdílet tuto složku** . Název sdílení ponechte jako *wmq*.

j) Klepněte na volbu **Oprávnění** > **Přidat ...**, a zadejte název globální skupiny *wmqha*. Klepněte na volbu **Zkontrolovat názvy** > **OK**.

k) Vyberte položku *wmqha* v seznamu **Názvy skupin nebo uživatelů**. Označte zaškrtávací políčko **Úplné řízení** v seznamu **Oprávnění pro *wmqha*** ; klepněte na tlačítko **Použít**.

l) Vyberte položku *Administrators* v seznamu **Názvy skupin nebo uživatelů**. Vyberte zaškrtávací políčko **Úplné řízení** v seznamu **Oprávnění pro *Administrátoři*** . klepněte na tlačítko **Použít** > **OK** > **OK** > **Zavřít**.

Jak pokračovat dále

Zkontrolujte, zda je možné číst a zapisovat soubory do sdílených adresářů z každého ze serverů IBM MQ . Zkontrolujte ID uživatele služby IBM MQ , *wmquser1* a interaktivní ID uživatele *wmquser2*.

1. Používáte-li vzdálenou pracovní plochu, musíte přidat *wmq**wmquser1* a *wmquser2* do lokální skupiny `Remote Desktop Users` na *mars*.

a. Přihlaste se k produktu *mars* jako *wmq*\`Administrator`

b. Spuštěním příkazu **lusrmgr.msc** otevřete okno Lokální uživatelé a skupiny.

c. Klepněte na volbu **Skupiny**. Klepněte pravým tlačítkem myši na volbu **Uživatelé vzdálené pracovní plochy** > **Vlastnosti** > **Přidat ...**. Zadejte *wmquser1 ; wmquser2* a klepněte na **Kontrolovat názvy**.

d. Zadejte jméno uživatele a heslo administrátora domény, *wmq*\`Administratora` klepněte na tlačítko **OK** > **Použít** > **OK**.

e. Zavřete okno Lokální uživatelé a skupiny.

2. Přihlaste se k produktu *mars* jako *wmq**wmquser1*.

a. Otevřete okno produktu Windows Explorer a zadejte příkaz *\\sun\wmq*.

Systém odpoví otevřením podílu portálu *wmq* na systému *sun.wmq.example.com*a vypíše seznam adresářů dat a protokolů.

b. Zkontrolujte oprávnění produktu *wmquser1* tak, že vytvoříte soubor v podadresáři dat, přidáte nějaký obsah, že jej budete číst a pak jej vymažete.

3. Přihlaste se k produktu *mars* jako *wmq\wmquser2*a zopakujte kontrolu.
4. Proveďte další úlohu, abyste vytvořili správce front pro použití sdílených dat a adresářů protokolu, viz "Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení" na stránce 474.

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, které jsou autorizovány alternativní globální skupinou zabezpečení

Windows *Čtení a zápis sdílených dat a souborů protokolu, které jsou autorizovány alternativní globální skupinou zabezpečení*

Tato úloha ukazuje, jak použít parametr -a u příkazu **crtmqm** . Příznak -a poskytuje správci front přístup k příslušným protokorovým souborům a datovým souborům ve vzdáleném sdílení souborů pomocí alternativní skupiny zabezpečení.

V konfiguraci škálování produkce možná budete muset upravit konfiguraci na existující doménu. Například můžete definovat různé skupiny domén pro autorizaci různých sdílených prostředků a pro seskupení ID uživatelů, kteří spouštějí správce front.

Příklad konfigurace se skládá ze tří serverů:

sun
Řadič domény produktu Windows Server 2008. Je vlastníkem domény *wmq.example.com* , která obsahuje *Sun*, *mars*a *venus*. Pro účely ilustrace se používá také jako souborový server.

mars
Server Windows Server 2008 použitý jako první server IBM MQ . Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

venus
Server Windows Server 2008 používaný jako druhý server IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

Postupujte podle kroků uvedených v následujících úlohách. Úlohy vytvoří řadič domény a doménu, nainstalujte produkt IBM MQ for Windows na jeden server a vytvořte sdílení souboru pro data a soubory protokolu. Pokud konfigurujete existující řadič domény, můžete zjistit, že je užitečné vyzkoušet si kroky na novém serveru Windows Server 2008. Kroky je možné upravit podle své domény.

1. "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 465.
2. "Instalace produktu IBM MQ na server nebo pracovní stanici v doméně Windows" na stránce 469.
3. "Vytvoření sdíleného adresáře pro data správce front a soubory protokolu v systému Windows" na stránce 471.

Informace o této úloze

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů

protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 461.

V této úloze vytvoříte správce front, ve kterém jsou uložena data a protokoly ve vzdáleném adresáři na souborovém serveru. Pro účely tohoto příkladu je souborový server stejným serverem jako řadič domény. Adresář obsahující data a složky protokolu je sdílen s úplným oprávněním pro řízení, které je poskytnuto globální skupině wmqha.

Postup

1. Přihlaste se k serveru domény, *mars*jako lokální administrátor, *mars*\Administrator.
2. Otevřte příkazové okno.
3. Restartujte službu IBM MQ .

   Službu musíte restartovat, aby ID uživatele, pod kterým je spuštěna, získalo další pověření zabezpečení, která jste pro ni nakonfigurovali.

   Zadejte příkazy:

   ```
   endmqsvc
   strmqsvc
   ```

   Odezvy systému:

   ```
   5724-H72 (C) Copyright IBM Corp. 1994, 2024.  ALL RIGHTS RESERVED.
   The MQ service for installation 'Installation1' ended successfully.
   ```

   A:

   ```
   5724-H72 (C) Copyright IBM Corp. 1994, 2024.  ALL RIGHTS RESERVED.
   The MQ service for installation 'Installation1' started successfully.
   ```
4. Vytvořte správce front.

   ```
   crtmqm -a wmq\wmqha -sax -u SYSTEM.DEAD.LETTER.QUEUE -md \\sun\wmq\data -ld \\sun\wmq\logs
   QMGR
   ```

   Musíte zadat doménu, *wmq*, alternativní skupiny zabezpečení *wmqha* uvedením úplného názvu domény globální skupiny *"wmq\wmqha"*.

   Musíte vyhláskovat název UNC (Universal Naming Convention) pro sdílení *\\sun\wmq*a nepoužívat odkaz na mapovaný disk.

   Odezva systému:

   ```
   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 s více instancemi na řadičích domény Windows*

Příklad ukazuje, jak nastavit správce front s více instancemi na Windows na řadičích domény. Nastavení demonstruje zahrnuté koncepce, spíše než aby bylo produkční měřítko. Tento příklad je založen na serveru Windows Server 2008. Tyto kroky se mohou lišit od dalších verzí serveru Windows .

Konfigurace používá koncept mini-domény nebo "domainlet" ; Viz uzly klastru Windows 2000, Windows Server 2003 a Windows Server 2008 jako řadiče domény. Chcete-li do existující domény přidat správce front s více instancemi, přečtěte si téma “Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462.

Příklad konfigurace se skládá ze tří serverů:

sun
Server Windows Server 2008 používaný jako první řadič domény. Definuje doménu *wmq.example.com* , která obsahuje *sun*, *earth*a *mars*. Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

earth
Server Windows Server 2008 používaný jako druhý server řadiče domény IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

mars
Server Windows Server 2008 používaný jako souborový server.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. V systému Windowsnení nutné ověřovat systém souborů, do kterého chcete ukládat data správce front a soubory žurnálu. Procedura kontroly, Ověření chování sdíleného systému souborů, je použitelná pro UNIX and Linux. V systému Windowsjsou kontroly vždy úspěšné.

2. Chcete-li vytvořit první řadič domény, proveďte kroky v části "Vytvoření Active Directory a domény DNS v systému Windows" na stránce 465 .
3. Chcete-li přidat druhý řadič domény, nainstalujte produkt IBM MQ for Windows na oba řadiče domény a ověřte instalaci pomocí kroků uvedených v tématu "Přidání druhého řadiče domény Windows do vzorové domény" na stránce 481 .
4. Proveďte kroky uvedené v části "Instalace produktu IBM MQ na řadičích domény Windows v ukázkové doméně" na stránce 482 a nainstalujte produkt IBM MQ na dva řadiče domény.

Informace o této úloze

Na souborovém serveru ve stejné doméně vytvořte sdílené adresáře pro protokol správce front a datové adresáře. Dále vytvořte první instanci správce front s více instancemi, který používá sdílení souboru na jednom z řadičů domény. Vytvořte druhou instanci na jiném řadiči domény a nakonec ověřte konfiguraci. Můžete vytvořit sdílení souboru na řadiči domény.

V ukázce je *sun* prvním řadičem domény, *earth* druhým a *mars* je souborový server.

Postup

1. Vytvořte adresáře, které budou obsahovat data správce front a soubory protokolu.
   a) V systému *mars*zadejte příkaz:

```
md c:\wmq\data , c:\wmq\logs
```

2. Sdílejte adresáře, které mají obsahovat data správce front a soubory protokolu.

   Musíte povolit úplný přístup k řízení přístupu k lokální skupině domén `mqma` ID uživatele, které používáte k vytvoření správce front. V tomto příkladu mají ID uživatelů, kteří jsou členy produktu `Domain Administrators` , oprávnění k vytváření správců front.

   Sdílení souboru musí být na serveru, který je ve stejné doméně jako řadiče domény. V tomto příkladě je server *mars* ve stejné doméně jako řadiče domény.

   a) V produktu Windows Explorer klepněte pravým tlačítkem myši na ***c: \wmq*** > **Vlastnosti**.
   b) Klepněte na kartu **Zabezpečení** a klepněte na volbu **Rozšířené** > **Upravit ...**.
   c) Zrušte označení zaškrtávacího políčka **Zahrnout oprávnění k dědičné oprávnění u vlastníka tohoto objektu**. Klepněte na tlačítko **Kopírovat** v okně Zabezpečení produktu Windows .
   d) Vyberte řádky pro uživatele v seznamu **Položky oprávnění** a klepněte na tlačítko **Odebrat**. Řádky pro SYSTEM, Administrators a CREATOR OWNER ponechejte v seznamu **Položky oprávnění**.
   e) Klepněte na tlačítko **Přidat ...**. a zadejte název lokální skupiny domén *mqm*. Klepněte na **Kontrolovat názvy**
   f) Jako odpověď na okno zabezpečení produktu Windows zadejte název a heslo produktu `Domain Administrator` a klepněte na tlačítko **OK** > **OK**.
   g) V okně Položka oprávnění pro `wmq` vyberte **Úplné řízení** v seznamu **Oprávnění**.
   h) Klepněte na tlačítko **OK** > **Použít** > **OK** > **OK** > **OK**
   i) Opakujte kroky e až h , chcete-li přidat `Domain Administrators`.
   j) V produktu Windows Explorer klepněte pravým tlačítkem myši na ***c: \wmq*** > **Sdílet ...**.
   k) Klepněte na volbu **Rozšířené sdílení ...** a vyberte zaškrtávací políčko **Sdílet tuto složku** . Název sdílení ponechte jako *wmq*.
   l) Klepněte na volbu **Oprávnění** > **Přidat ...**, a zadejte název lokální skupiny domén *mqm* ; `Domain Administrators`. Klepněte na volbu **Kontrolovat názvy**.
   m) Jako odpověď na okno zabezpečení produktu Windows zadejte název a heslo produktu `Domain Administrator` a klepněte na tlačítko **OK** > **OK**.
3. Vytvořte správce front *QMGR* na prvním řadiči domény *sun*.

```
crtmqm -sax -u SYSTEM.DEAD.LETTER.QUEUE -md \\mars\wmq\data -ld \\mars\wmq\logs QMGR
```

Odezva systému:

```
IBM MQ queue manager created.
Directory '\\mars\wmq\data\QMGR' created.
The queue manager is associated with installation 'Installation1'.
Creating or replacing default objects for queue manager 'QMGR'.
Default objects statistics : 74 created. 0 replaced. 0 failed.
Completing setup.
Setup completed.
```

4. Spusťte správce front v systému *sun*tak, že povolíte instanci v pohotovostním režimu.

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'QMGR' during the log
replay phase.
Log replay for queue manager 'QMGR' complete.
Transaction manager state recovered for queue manager 'QMGR'.
IBM MQ queue manager 'QMGR' started using V7.1.0.0.
```

5. Vytvořte druhou instanci produktu *QMGR* v systému *earth*.
   a) Zkontrolujte hodnoty parametrů Předpona a InstallationName , které jsou správné pro produkt *earth*.

      V systému *sun*spusťte příkaz **dspmqinf** :

      ```
      dspmqinf QMGR
      ```

      Odezva systému:

      ```
      QueueManager:
      Name=QMGR
      Directory=QMGR
      Prefix=C:\ProgramData\IBM\MQ
      DataPath=\\mars\wmq\data\QMGR
      InstallationName=Installation1
      ```

   b) Okopírujte strojově čitelnou formu stanzy **QueueManager** do schránky.

      V systému *sun* spusťte příkaz **dspmqinf** znovu s parametrem -o command .

      ```
      dspmqinf -o command QMGR
      ```

      Odezva systému:

      ```
      addmqinf -s QueueManager -v Name=QMGR
      -v Directory=QMGR -v Prefix="C:\ProgramData\IBM\MQ"
      -v DataPath=\\mars\wmq\data\QMGR
      ```

c) V systému *earth* spusťte příkaz **addmqinf** ze schránky a vytvořte instanci správce front v systému *earth*.

V případě potřeby upravte příkaz tak, aby vyhovoval rozdílům v parametrech Předpona nebo InstallationName .

```
addmqinf -s QueueManager -v Name= QMGR
-v Directory= QMGR -v Prefix="C:\Program Files\IBM\WebSphere MQ"
-v DataPath=\\mars\wmq\data\QMGR
```

```
IBM MQ configuration information added.
```

6. Spusťte instanci v pohotovostním režimu správce front v systému *earth*.

```
strmqm -x QMGR
```

Odezva systému:

```
IBM MQ queue manager 'QMGR' starting.
The queue manager is associated with installation 'Installation1'.
A standby instance of queue manager 'QMGR' has been started. The active
instance is running elsewhere.
```

Výsledky

Ověřte, zda se správce front přepne z *sun* na *earth*:

1. V systému *sun*spusťte příkaz:

```
endmqm -i -r -s QMGR
```

Odezva systému na *sun*:

```
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ending.
IBM MQ queue manager 'QMGR' ended, permitting switchover to
a standby instance.
```

2. U *earth* opakovaně zadejte příkaz:

```
dspmq
```

Systémové odezvy:

```
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running as standby)
QMNAME(QMGR) STATUS(Running)
```

Jak pokračovat dále

Chcete-li ověřit správce front s více instancemi pomocí ukázkových programů, přečtěte si téma “Ověření správce front s více instancemi v systému Windows” na stránce 485.

Související úlohy

“Přidání druhého řadiče domény Windows do vzorové domény” na stránce 481

“Instalace produktu IBM MQ na řadičích domény Windows v ukázkové doméně” na stránce 482

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* za účelem vytvoření domény Windows , ve které se mají spouštět správce front s více instancemi na řadičích domény a na souborových serverech.

Příklad konfigurace se skládá ze tří serverů:

sun
Server Windows Server 2008 používaný jako první řadič domény. Definuje doménu *wmq.example.com* , která obsahuje *sun*, *earth*a *mars*. Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

earth
Server Windows Server 2008 používaný jako druhý server řadiče domény IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

mars
Server Windows Server 2008 používaný jako souborový server.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li vytvořit řadič domény, *sun*pro doménu *wmq.example.com*, proveďte kroky v části “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465 . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
2. Nainstalujte produkt Windows Server 2008 na server ve výchozí pracovní skupině, WORKGROUP. Pro tento příklad je server pojmenován *earth*.

Informace o této úloze

V této úloze nakonfigurujete server Windows Server 2008 s názvem *earth*jako druhý řadič domény v doméně *wmq.example.com* .

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 461.

Postup

1. Přidejte řadič domény, *sun.wmq.example.com* do *earth* jako server DNS.
   a) V produktu *earth*se přihlaste jako *earth*\Administrator a klepněte na tlačítko **Spustit**.
   b) Klepněte pravým tlačítkem myši na **Síť** > **Vlastnosti** > **Spravovat síťová připojení**.
   c) Klepněte pravým tlačítkem myši na síťový adaptér a poté klepněte na volbu **Vlastnosti**.

      Systém odpoví v okně Vlastnosti připojení k místní síti, které uvádí položky, které připojení používá.
   d) Ze seznamu položek v okně Vlastnosti připojení lokální oblasti vyberte ze seznamu položek **Internet Protocol verze 4** nebo **Internet Protocol verze 6** . Klepněte na volbu **Vlastnosti** > **Rozšířené ...** a klepněte na kartu **DNS** .
   e) Pod adresou serveru DNS klepněte na **Přidat ...**.
   f) Zadejte adresu IP řadiče domény, který je také serverem DNS, a klepněte na tlačítko **Přidat**.
   g) Klepněte na volbu **Připojit tyto přípony systému DNS** > **Přidat ...**.

h) Zadejte *wmq.example.com* a klepněte na **Přidat**.

i) Zadejte *wmq.example.com* do pole **Přípona systému DNS pro toto připojení** .

j) Vyberte volbu **Registrovat tuto adresu připojení v DNS** a **Použít příponu tohoto připojení v registraci DNS**. Klepněte na tlačítko **OK** > **OK** > **Zavřít** .

k) Otevřete příkazové okno a zadejte příkaz **ipconfig /all** , abyste zkontrolli nastavení TCP/IP.

2. Přihlaste se k řadiči domény *sun*jako administrátor lokálního systému nebo administrátor produktu `Workgroup` .

   Je-li server již konfigurován jako řadič domény, musíte se přihlásit jako administrátor domény.

3. Spusťte průvodce Active Directory Domain Services.

   a) Klepněte na nabídku **Start** > **Spustit ...** Zadejte `dcpromo` a klepněte na **OK**.

   Nejsou-li binární soubory Active Directory již nainstalovány, produkt Windows nainstaluje soubory automaticky.

4. Konfigurujte *earth* jako druhý řadič domény v doméně *wmq.example.com* .

   a) V prvním okně průvodce ponechte zaškrtávací políčko **Použít rozšířenou instalaci režimu** prázdné. Klepněte na tlačítko **Další** > **Další** a klepněte na volbu **Vytvořit přidat řadič domény do existující domény** > **Další**.

   b) Zadejte *wmq* do pole **Zadejte název libovolné domény v tomto lese ...** . Klepnete-li na přepínač **Alternativní pověření** , klepněte na **Nastavit ...**. Zadejte jméno a heslo administrátora domény a klepněte na tlačítko **OK** > **Další** > **Další** > **Další**.

   c) V okně Další volby řadiče domény přijměte volby **Server DNS** a **Globální katalog** , které jste vybrali. Klepněte na tlačítko **Další** > **Další**.

   d) Na heslo administrátora režimu obnovy adresářových služeb zadejte heslo do polí **Heslo** a **Potvrdit heslo** a klepněte na tlačítko **Další** > **Další**.

   e) Když jste vyzváni k zadání **Síťových pověření**, zadejte heslo administrátora domény. V závěrečném okně průvodce vyberte volbu **Znovu spustit po dokončení** .

   f) Po nějakou dobu se může okno otevřít s chybou **DCPromo** týkající se delegování DNS; klepněte na tlačítko **OK**. Server znovu zavede systém.

Výsledky

Po opětném zavedení systému *earth* se přihlaste jako administrátor domény. Zkontrolujte, zda byla doména `wmq.example.com` replikována na *earth*.

Jak pokračovat dále

Pokračujte instalací produktu IBM MQ ; viz “Instalace produktu IBM MQ na řadičích domény Windows v ukázkové doméně” na stránce 482.

Související úlohy

Windows Instalace produktu IBM MQ na řadičích domény Windows v ukázkové doméně

“Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465

Windows *Instalace produktu IBM MQ na řadičích domény Windows v ukázkové doméně*

Nainstalujte a nakonfigurujte instalace produktu IBM MQ na obou řadičích domény v doméně *wmq.example.com* .
Sem zadejte krátký popis; použije se pro první odstavec a abstrakt.

Příklad konfigurace se skládá ze tří serverů:

sun
Server Windows Server 2008 používaný jako první řadič domény. Definuje doménu *wmq.example.com* , která obsahuje *sun*, *earth*a *mars*. Obsahuje jednu instanci správce front pro více instancí s názvem *QMGR*.

earth
Server Windows Server 2008 používaný jako druhý server řadiče domény IBM MQ . Obsahuje druhou instanci správce front pro více instancí s názvem *QMGR*.

mars
Server Windows Server 2008 používaný jako souborový server.

Nahraďte kurzívou názvy v příkladu názvy dle vašeho výběru.

Než začnete

1. Chcete-li vytvořit řadič domény, *sun*pro doménu *wmq.example.com*, proveďte kroky v části “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465 . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
2. Chcete-li vytvořit druhý řadič domény, *earth*, pro doménu *wmq.example.com*, proveďte kroky v části “Přidání druhého řadiče domény Windows do vzorové domény” na stránce 481 . Změňte kurzívu tak, aby vyhovovala vaší konfiguraci.
3. Informace o dalších verzích produktu Windows , na kterých lze spustit produkt IBM MQ , najdete v tématu Hardwarové a softwarové požadavky na systémech Windows .

Informace o této úloze

Nainstalujte a nakonfigurujte instalace produktu IBM MQ na obou řadičích domény v doméně *wmq.example.com* .

Postup

1. Nainstalujte IBM MQ na *sun* a *earth*.

   Další informace o spuštění průvodce instalací produktu IBM MQ for Windows naleznete v tématu Instalace serveru IBM MQ v systému Windows .

   a) V systémech *sun* a *earth*se přihlaste jako administrátor domény *wmq*\Administrator.

   b) Spusťte příkaz **Setup** na instalačním médiu produktu IBM MQ for Windows .

      Spustí se příruční panel produktu IBM MQ .

   c) Klepněte na **Softwarové požadavky** , chcete-li zkontrolovat, zda je nainstalován předem vyžadovaný software.

   d) Klepněte na volbu **Konfigurace sítě** > **Ne**.

      Můžete konfigurovat buď ID uživatele domény, nebo ne pro tuto instalaci. ID uživatele, který se vytvoří, je ID lokálního uživatele domény.

   e) Klepněte na volbu **IBM MQ Instalace**, vyberte jazyk instalace a klepněte na volbu Spustit instalační program produktu IBM MQ .

   f) Potvrďte licenční smlouvu a klepněte na tlačítko **Další** > **Další** > **Instalovat** , chcete-li přijmout výchozí konfiguraci. Čekejte, až se instalace dokončí, a klepněte na tlačítko **Dokončit**.

      Chcete-li změnit název instalace, instalovat různé komponenty, konfigurovat jiný adresář pro data správce front a protokoly nebo instalovat do jiného adresáře, klepněte na volbu **Vlastní** namísto volby **Typická**.

      Produkt IBM MQ je instalován a instalační program spustí průvodce "Příprava produktu IBM MQ " .

   Instalace produktu IBM MQ for Windows nakonfiguruje lokální skupinu domén mqma skupinu domén Domain mqm. Domain mqm je členem mqm. Následné řadiče domény ve stejné doméně sdílejí skupiny mqm a Domain mqm .

2. V produktu *earth* i v produktu *sun*spusťte "Průvodce přípravou produktu IBM MQ " .

   Další informace o spuštění průvodce "Příprava produktu IBM MQ " naleznete v tématu Konfigurace portálu IBM MQ pomocí Průvodce přípravou produktu IBM MQ.

a) Instalační program produktu IBM MQ spustí automaticky "Příprava produktu IBM MQ " .

Chcete-li průvodce spustit ručně, najděte zástupce složky "Prepare IBM MQ " ve složce **Start** > **Všechny programy** > **IBM MQ** . Vyberte zástupce, který odpovídá instalaci produktu IBM MQ v konfiguraci s více instalačními programy.

b) Click **Další** and leave **Ne.** clicked in response to the question "Identifikujte, zda v síti existuje řadič domény Windows 2000 nebo novější."[1].

c) Na poslední stránce průvodce zaškrtněte nebo zrušte zaškrtnutí zaškrtávacích políček podle potřeby a klepněte na tlačítko **Dokončit**.

Průvodce "Příprava produktu IBM MQ " vytvoří doménový lokální uživatel `MUSR_MQADMIN` na prvním řadiči domény a další lokální uživatele domény `MUSR_MQADMIN1` na druhém řadiči domény. Průvodce vytvoří službu IBM MQ na každém řadiči, s `MUSR_MQADMIN` nebo `MUSR_MQADMIN1` jako uživatele, který se přihlásí na službu.

3. Definujte uživatele, který má oprávnění k vytvoření správce front.

Uživatel musí mít právo přihlásit se lokálně a musí být členem lokální skupiny `mqm` domény. V řadičích domény nemají uživatelé domény právo přihlásit se lokálně, ale administrátoři ano. Při výchozím nastavení nemá žádný uživatel tyto atributy. V této úloze přidejte administrátory domény do lokální skupiny `mqm` domény.

a) Otevřete produkt **Server Manager** > **Role** > **Active Directory Domain Services** > ***wmq.example.com*** > **Users**.

b) Right-click **Administrátoři domény** > **Přidat do skupiny ...** a typu `mqm` ; klepněte na volbu **Zkontrolovat názvy** > **OK** > **OK**

Výsledky

1. Zkontrolujte, zda "Prepare IBM MQ " vytvořil uživatele domény, `MUSR_MQADMIN`:

   a. Otevřete produkt **Server Manager** > **Role** > **Active Directory Domain Services** > ***wmq.example.com*** > **Users**.

   b. Right-click **MUSR_MQADMIN** > **Vlastnosti ...** > **Člen**a uvidíte, že se jedná o člena `Domain users` a `mqm`.

2. Zkontrolujte, že produkt `MUSR_MQADMIN` má právo pracovat jako služba:

   a. Klepněte naKlepněte na nabídku **Start** > **Spustit ...**, Zadejte příkaz **`secpol.msc`** a klepněte na **OK**.

   b. Otevřete **Nastavení zabezpečení** > **Lokální zásady** > **Přiřazení uživatelských práv**. V seznamu zásad klepněte pravým tlačítkem myši na **Přihlásit se jako služba** > **Vlastnosti** a viz `MUSR_MQADMIN` se uvádí jako mající právo přihlásit se jako služba. Klepněte na tlačítko **OK**.

Jak pokračovat dále

1. Proveďte úlohu “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 492, abyste ověřili, že instalace a konfigurace fungují správně.
2. Přejděte zpět na úlohu “Vytvoření správce front s více instancemi na řadičích domény Windows” na stránce 477, abyste dokončili úlohu konfigurace správce front s více instancemi na řadičích domény.

Související úlohy

Windows Přidání druhého řadiče domény Windows do vzorové domény

Související odkazy

Uživatelská práva vyžadovaná pro službu IBM MQ Windows Service

[1] Můžete nakonfigurovat instalaci pro doménu. Vzhledem k tomu, že všichni uživatelé a skupiny na řadiči domény mají rozsah domény, neodlišujte se tím. Je jednodušší instalovat produkt IBM MQ , jako by se nenachází v doméně.

Windows *Ověření správce front s více instancemi v systému Windows*

Chcete-li ověřit konfiguraci správce front s více instancemi, použijte ukázkové programy **amqsghac**, **amqsphac** a **amqsmhac** . Toto téma nabízí vzorovou konfiguraci pro ověření konfigurace správce front s více instancemi na serveru Windows Server 2003.

Ukázkové programy s vysokou dostupností používají automatické opětovné připojení klienta. Dojde-li k selhání připojeného správce front, klient se pokusí znovu připojit ke správci front ve stejné skupině správců front. Popis ukázek, ukázkových programů vysoké dostupnosti, demonstruje opětovné připojení klienta pomocí správce front s jedinou instancí pro zjednodušení. Chcete-li ověřit konfiguraci správce front s více instancemi, můžete použít stejné ukázky s více správci front pro více instancí.

Tento příklad používá konfiguraci s více instancemi popsanou v části “Vytvoření správce front s více instancemi na řadičích domény Windows” na stránce 477. Použijte konfiguraci k ověření, že správce front s více instancemi se přepne na instanci v pohotovostním režimu. Zastavte správce front pomocí příkazu **endmqm** a použijte volbu `-s`, switchover, option. Programy klienta se znovu připojí k nové instanci správce front a budou pokračovat v práci s novou instancí po mírném zpoždění.

Klient je instalován v obrazu 400 MB VMware , kde je spuštěn produkt Windows 7 Service Pack 1. Z bezpečnostních důvodů je připojen ke stejné síti hostitele VMware jako servery domén, na kterých běží správce front s více instancemi. Sdílí konfiguraci se složkou `/MQHA` , která obsahuje tabulku připojení klienta, a zjednodušíte tak konfiguraci.

Ověření překonání selhání pomocí produktu IBM MQ Explorer

Před použitím ukázkových aplikací k ověření překonání selhání spusťte program IBM MQ Explorer na každém serveru. Přidejte obě instance správce front do každého průzkumníku pomocí průvodce **Přidat vzdáleného správce front > Připojit přímo k víceinstanceinstanční správci front** . Ujistěte se, že obě instance jsou spuštěny, což umožňuje pohotovostní režim. Zavřete okno se spuštěnou instancí VMware s aktivní instancí, virtuálně vypněte server nebo zastavte aktivní instanci, což umožňuje přepnutí na záložní instanci a opětovné připojení klientů k opětovnému připojení.

Upozornění: Vypnete-li server, ujistěte se, že se nejedná o adresář, který je hostitelem složky `MQHA` !

Poznámka: Volba **Povolit přepnutí na instanci v pohotovostním režimu** nemusí být k dispozici v dialogovém okně **Zastavit správce front** . Volba chybí, protože správce front je spuštěn jako správce front s jednou instancí. Musíte je spustit bez volby **Povolit instanci v pohotovostním režimu** . Pokud je váš požadavek na zastavení správce front odmítnut, podívejte se do okna **Podrobnosti** , pravděpodobně není spuštěna žádná instance v pohotovostním režimu.

Ověření překonání selhání pomocí ukázkových programů

Zvolte server, na kterém má být spuštěna aktivní instance.

Je možné, že jste zvolili jeden ze serverů pro hostování adresáře `MQHA` nebo systému souborů. Pokud plánujete otestovat překonání selhání zavřením okna VMware se spuštěným aktivním serverem, ujistěte se, že to není ten, který hostuje `MQHA` !

Na serveru, na kterém je spuštěna aktivní instance správce front

1. Upravte hodnoty *ipaddr1* a *ipaddr2* a uložte následující příkazy v produktu `N:\hasample.tst.` .

```
DEFINE QLOCAL(SOURCE) REPLACE
DEFINE QLOCAL(TARGET) REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(SVRCONN)  TRPTYPE(TCP) +
MCAUSER(' ') REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNAME(' ipaddr1 (1414), ipaddr2 (1414)') QMNAME(QM1) REPLACE
START CHANNEL(CHANNEL1)
DEFINE LISTENER(LISTENER.TCP) TRPTYPE(TCP) CONTROL(QMGR)
DISPLAY LISTENER(LISTENER.TCP) CONTROL
DISPLAY LSSTATUS(LISTENER.TCP) STATUS
```

Poznámka: Pokud ponecháte parametr **MCAUSER** prázdný, odešle se klientovi ID uživatele klienta. ID uživatele klienta musí mít na serverech správná oprávnění. Alternativou je nastavit parametr **MCAUSER** v kanálu SVRCONN na ID uživatele, které jste nakonfigurovali na serveru.

2. Otevřete příkazový řádek s cestou `N:\` a spusťte příkaz:

```
runmqsc -m QM1 < hasample.tst
```

3. Ověřte, zda je modul listener spuštěný a má-li řízení správce front, a to buď kontrolou výstupu příkazu **runmqsc** .

```
LISTENER(LISTENER.TCP)CONTROL(QMGR)
LISTENER(LISTENER.TCP)STATUS(RUNNING)
```

Nebo pomocí IBM MQ Explorer , který spouští modul listener protokolu TCP/IP, a má `Control = Queue Manager`.

Na klientu

1. Namapujte sdílený adresář `C:\MQHA` na serveru na `N:\` na straně klienta.
2. Otevřete příkazový řádek s cestou `N:\`. Nastavte proměnnou prostředí `MQCHLLIB` tak, aby ukazovala na tabulku definic kanálů klienta (CCDT) na serveru:

```
SET MQCHLLIB=N:\data\QM1\@ipcc
```

3. Na příkazový řádek zadejte příkazy:

```
start amqsghac TARGET QM1
start amqsmhac -s SOURCE -t TARGET -m QM1
start amqsphac SOURCE QM1
```

Poznámka: Máte-li problémy, spusťte aplikace na příkazovém řádku tak, aby kód příčiny byl vytištěn na konzole, nebo se podívejte na AMQERR01.LOG ve složce `N:\data\QM1\errors` .

Na serveru, na kterém je spuštěna aktivní instance správce front

1. Proveďte jednu z následujících akcí:
   - Zavřete okno se spuštěnou instancí serveru VMware s obrazem aktivního serveru.
   - Pomocí konzoly IBM MQ Explorerzastavte aktivní instanci správce front, což umožňuje přepnutí do instance v pohotovostním režimu a instruující se znovu připojitelné klienty k opětovnému připojení.
2. Tři klienti nakonec zjistí, že spojení je přerušeno, a pak se znovu připojí. V této konfiguraci, pokud zavřete okno serveru, trvá přibližně sedm minut, než se znovu ustanoví všechna tři připojení. Některá spojení se znovu ustanoví dobře před ostatními.

Výsledky

```
N:\>amqsphac SOURCE QM1
Sample AMQSPHAC start
target queue is SOURCE
message Message 1
message Message 2
message Message 3
message Message 4
message Message 5
17:05:25 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message Message 6
message Message 7
message Message 8
message Message 9
```

```
N:\>amqsmhac -s SOURCE -t TARGET -m QM1
Sample AMQSMHA0 start

17:05:25 : EVENT : Connection Reconnecting (Delay: 97ms)
17:05:48 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:53 : EVENT : Connection Reconnected
```

```
N:\>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 dat správce sdílených front a adresářů protokolů a souborů v systému Windows*

Toto téma popisuje, jak můžete zabezpečit sdílené umístění pro data správce front a soubory žurnálu pomocí globální alternativní skupiny zabezpečení. Můžete sdílet umístění mezi různými instancemi správce front spuštěnými na různých serverech.

Obvykle nenastavíte sdílené umístění pro data správce front a soubory protokolu. Když instalujete produkt IBM MQ for Windows, instalační program vytvoří domovský adresář dle vašeho výběru pro všechny správce front, kteří jsou na tomto serveru vytvoři. Zazabezpečuje adresáře s lokální skupinou `mqm` a konfiguruje ID uživatele pro službu IBM MQ pro přístup k adresářům.

Když zabezpečujete sdílenou složku se skupinou zabezpečení, musí mít uživatel, který má oprávnění pro přístup ke složce, pověření skupiny. Předpokládejme, že složka na vzdáleném souborovém serveru je zabezpečena pomocí lokální skupiny `mqm` na serveru s názvem *`mars`*. Učinit uživatele, který spouští správce front, zpracovávat člena lokální skupiny `mqm` v systému *`mars`*. Uživatel má pověření, která odpovídají pověření složky na vzdáleném souborovém serveru. Pomocí těchto pověření je správce front schopen přistupovat k příslušným datům a protokoluje soubory ve složce. Uživatel, který spouští procesy správce front na jiném serveru, je členem jiné lokální skupiny produktu `mqm` , která nemá odpovídající pověření. Pokud správce front běží na jiném serveru než portál *`mars`*, nebude mít přístup k datům a souborům protokolu, které vytvořil, když běžel na serveru *`mars`*. I v případě, že uživatel domény uživatel domény, má jiná pověření, protože musí získat pověření z lokální skupiny `mqm` v systému *`mars`*a to nemůže provést z jiného serveru.

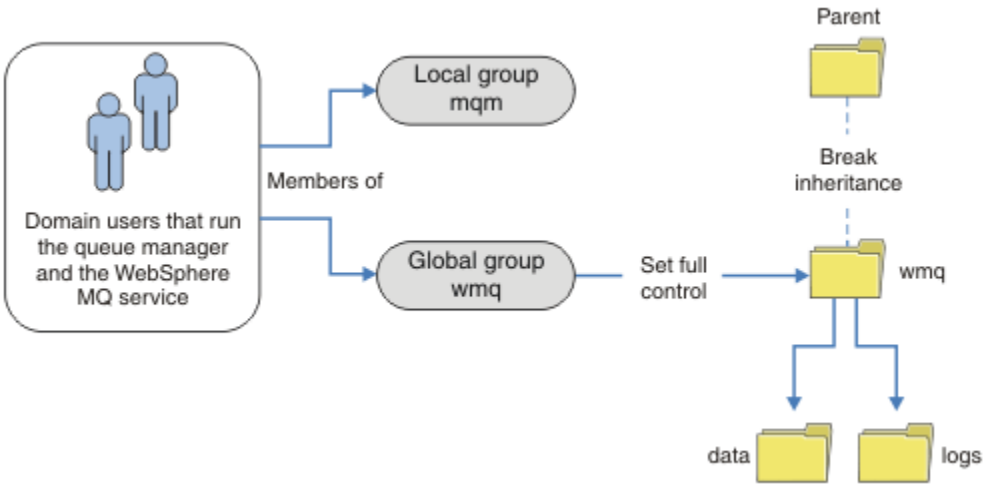
Zadání správce front s globální alternativní skupinou zabezpečení tento problém řeší; viz Obrázek 76 na stránce 488. Zabezpečte vzdálenou složku s globální skupinou. Když jej vytvoříte v systému *mars*, předejte název globální skupiny ke správci front. Předejte název globální skupiny jako alternativní skupinu zabezpečení pomocí parametru `-a [ r]` u příkazu **crtmqm** . Pokud přenesete správce front tak, aby byl spuštěn na jiném serveru, je název skupiny zabezpečení přenesen s tímto názvem. Název je přenesen ve stanze **AccessMode** v souboru `qm.ini` jako `SecurityGroup` . například:

```
AccessMode:
SecurityGroup=wmq\wmq
```

Stanza **AccessMode** v `qm.ini` obsahuje také `RemoveMQMAccess` ; například:

```
AccessMode:
RemoveMQMAccess=true|false
```

Je-li tento atribut zadán s hodnotou `true`a byla poskytnuta také skupina přístupů, lokální skupina mqm nemá udělen přístup k datovým souborům správce front.

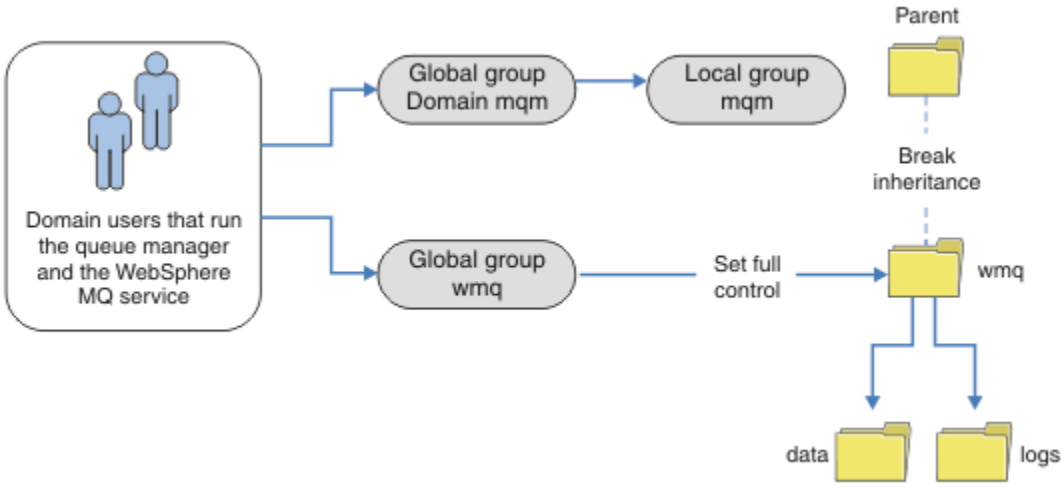


Obrázek 76. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (1)

Pro ID uživatele, kterým se mají spustit procesy správce front, mají-li mít odpovídající pověření globální skupiny zabezpečení, musí mít ID uživatele také globální rozsah. Nemůžete vytvořit lokální skupinu nebo činitele jako člena globální skupiny. V produktu Obrázek 76 na stránce 488se uživatelům, kteří spouštějí procesy správce front, zobrazují jako uživatelé domény.

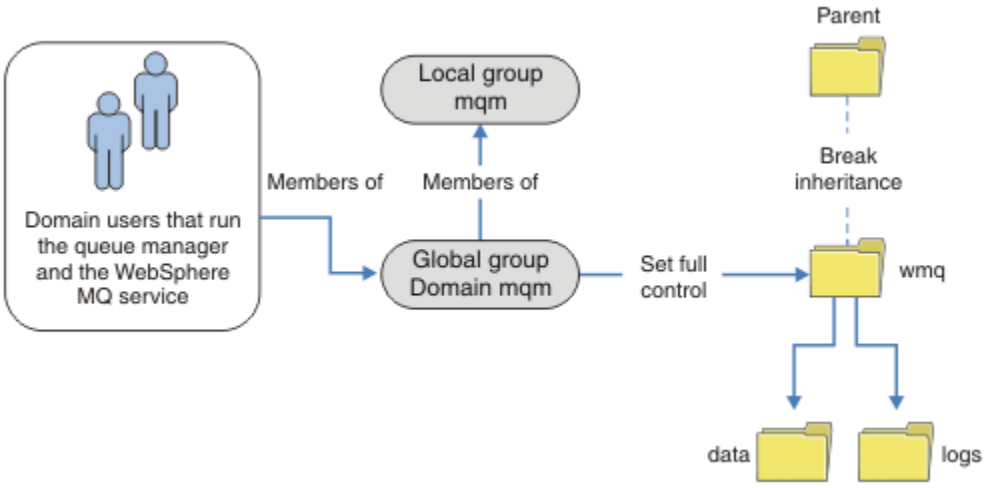
Pokud implementujete mnoho serverů IBM MQ , seskupení uživatelů v produktu Obrázek 76 na stránce 488 není vhodné. Budete muset opakovat proces přidání uživatelů do lokálních skupin pro každý server IBM MQ . Namísto toho vytvořte na řadiči domény globální skupinu `Domain mqm` a vytvořte uživatele, kteří spouštějí členy IBM MQ skupiny `Domain mqm` , viz Obrázek 77 na stránce 489. Když instalujete produkt IBM MQ jako instalaci domény, průvodce "Příprava produktu IBM MQ " automaticky vytvoří skupinu `Domain mqm` za člena lokální skupiny `mqm` . Tytéž uživatelé jsou v obou globálních skupinách `Domain mqm` a `wmq`.

Tip: Tytéž uživatelé mohou spouštět produkt IBM MQ na různých serverech, ale na individuálním serveru musíte mít různé uživatele ke spuštění produktu IBM MQ jako služby a mohou být spuštěny interaktivně. Pro každou instalaci na serveru musíte mít také různé uživatele. Zpravidla proto `Domain mqm` obsahuje mnoho uživatelů.



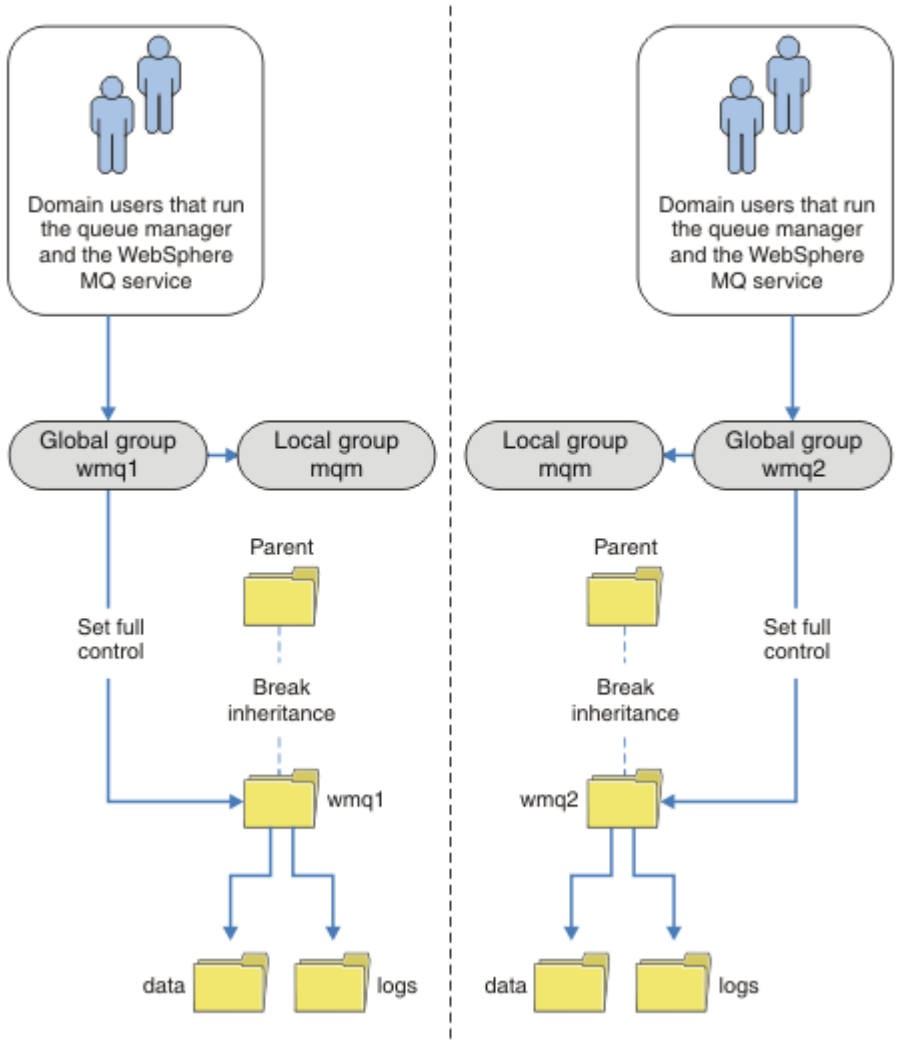
Obrázek 77. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (2)

Organizace v produktu Obrázek 77 na stránce 489 je zbytečně komplikovaná, jak stojí. Uspořádání má dvě globální skupiny se shodnými členy. Můžete zjednodušit organizaci a definovat pouze jednu globální skupinu; viz Obrázek 78 na stránce 489.



Obrázek 78. Zabezpečení dat správce front a protokolů pomocí alternativní globální skupiny zabezpečení (3)

Případně můžete potřebovat podrobnější úroveň řízení přístupu, kdy různí správci front omezeni na přístup k různým složkám. Další informace viz Obrázek 79 na stránce 490. V produktu Obrázek 79 na stránce 490jsou definovány dvě skupiny uživatelů domény v samostatných globálních skupinách za účelem zabezpečení různých protokolů správce front a datových souborů. Jsou zobrazeny dvě různé lokální skupiny `mqm` , které musí být na různých serverech IBM MQ . V tomto příkladu jsou správci front rozděleni do dvou sad s různými uživateli přidělenými na dvě sady. Tyto dvě sady mohou být testovacími a produkční správci front. Alternativní skupiny zabezpečení se nazývají `wmq1` a `wmq2`. Musíte ručně přidat globální skupiny `wmq1` a `wmq2` do příslušných správců front podle toho, zda se nacházejí v testovacím nebo výrobním oddělení. Konfigurace nemůže využít výhod, které instalace produktu IBM MQ šíří `Domain mqm` do lokální skupiny `mqm` jako v Obrázek 78 na stránce 489, protože existují dvě skupiny uživatelů.



Obrázek 79. Zabezpečení dat správce front a protokolů pomocí alternativního činitele globálního zabezpečení (4)

Alternativním způsobem rozdělení dvou oddělení na logické oblasti by bylo jejich umístění ve dvou doménách systému Windows. V takovém případě se můžete vrátit k použití jednoduššího modelu zobrazeného v produktu Obrázek 78 na stránce 489.

Windows *Zabezpečte nesdílená data správce front a adresáře a soubory protokolu v systému Windows*

Toto téma popisuje, jak můžete zabezpečit alternativní umístění pro data správce front a soubory protokolu, a to jak pomocí lokální skupiny `mqm` , tak i pomocí alternativní skupiny zabezpečení.

Typicky nenastavíte alternativní umístění pro data správce front a soubory protokolu. Když instalujete produkt IBM MQ for Windows, instalační program vytvoří domovský adresář dle vašeho výběru pro všechny správce front, které jsou vytvořeny. Zazabezpečuje adresáře s lokální skupinou `mqm` a konfiguruje ID uživatele pro službu IBM MQ pro přístup k adresářům.

Dva příklady demonstrují, jak nakonfigurovat řízení přístupu pro produkt IBM MQ. Příklady ukazují, jak vytvořit správce front se svými daty a protokoly v adresářích, které nejsou na datech a cestách protokolu vytvořených instalací. V prvním příkladu, “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 492, povolíte přístup k adresářům a adresářům protokolu tím, že udělíte oprávnění od lokální skupiny `mqm` . Druhý příklad, “Čtení a zápis dat a souborů protokolu autorizovaných alternativní lokální skupinou zabezpečení” na stránce 495, se liší v tom, že přístup k adresářům je autorizován alternativní skupinou zabezpečení. Když správce front přistupuje k adresářům pouze na jednom serveru, zabezpečení dat a souborů protokolu s alternativní skupinou zabezpečení

vám dává možnost zabezpečení různých správců front s různými lokálními skupinami nebo činiteli. Při přístupu k adresářům pomocí správce front spuštěného na různých serverech, jako je správce front s více instancemi, je jediným výběrem volby zabezpečení dat a souborů žurnálu s alternativní skupinou zabezpečení. Další informace naleznete v tématu “Zabezpečení dat správce sdílených front a adresářů protokolů a souborů v systému Windows” na stránce 487.

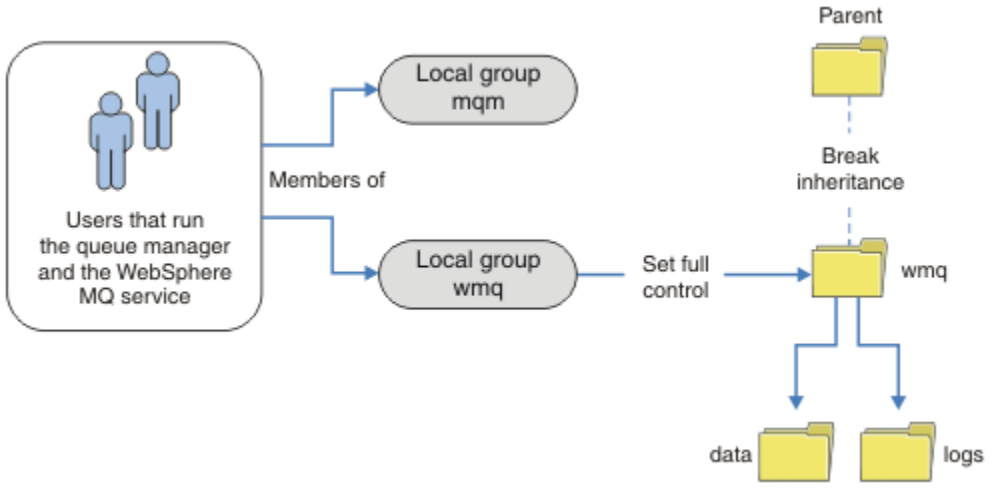
Konfigurace oprávnění zabezpečení dat správce front a souborů protokolu není běžná úloha v produktu Windows. Když instalujete produkt IBM MQ for Windows, buď zadejte adresáře pro data a protokoly správce front, nebo přijměte výchozí adresáře. Instalační program automaticky zabezpečuje tyto adresáře s lokální skupinou `mqm` a poskytuje jí úplné oprávnění k řízení. Proces instalace zajišťuje, že ID uživatele, který spouští správce front, je členem lokální skupiny `mqm` . Ostatní přístupová oprávnění k adresářům můžete upravit tak, aby odpovídala vašim požadavkům na přístup.

Přesunete-li data a adresář souborů protokolu do nových umístění, musíte nakonfigurovat zabezpečení nových umístění. Umístění těchto adresářů můžete změnit, pokud zálohujete správce front a obnovíte jej na jiný počítač nebo pokud změníte správce front tak, aby byl správcem front s více instancemi. Máte možnost výběru dvou způsobů, jak zabezpečit data správce front a adresáře protokolů ve svém novém umístění. Adresáře můžete zabezpečit omezením přístupu k lokální skupině `mqm` , nebo můžete omezit přístup k libovolné skupině zabezpečení dle vašeho výběru.

Potrvá nejméně několik kroků k zabezpečení adresářů pomocí lokální skupiny produktu `mqm` . Nastavte oprávnění k datům a adresářům protokolu tak, aby umožňovala plnou kontrolu celé skupiny produktu `mqm` . Typickým přístupem je kopírovat existující sadu oprávnění a odebrat dědičnost z nadřízené položky. Oprávnění jiných činitelů pak můžete odebrat nebo omezit.

Spustíte-li správce front pod jiným ID uživatele do služby vytvořené pomocí průvodce přípravou produktu IBM MQ , musí být toto ID uživatele členem lokální skupiny `mqm` . Úloha “Čtení a zápis dat a souborů protokolu autorizovaných lokální skupinou mqm” na stránce 492vás provede jednotlivými kroky.

Data správce front a soubory protokolu můžete také zabezpečit pomocí alternativní skupiny zabezpečení. Proces zabezpečení dat správce front a souborů žurnálu s alternativní skupinou zabezpečení má řadu kroků, které odkazují na produkt Obrázek 80 na stránce 491. Jako příklad alternativní skupiny zabezpečení je použita lokální skupina `wmq`.



Obrázek 80. Zabezpečení dat správce front a protokolů pomocí alternativní lokální skupiny zabezpečení, wmq

1. Buď vytvořte samostatné adresáře pro data a protokoly správce front, společný adresář nebo společný nadřízený adresář.
2. Zkopírujte existující sadu zděděných oprávnění pro adresáře nebo nadřízený adresář a upravte je podle svých potřeb.

3. Zabezpečte adresáře, které mají obsahovat správce front a protokoly, a to tak, že dáte alternativní skupině, wmq, plnou kontrolu oprávnění k adresářům.
4. Udělit oprávnění všech ID uživatelů, která spouštějí správce front, zpracuje pověření alternativní skupiny zabezpečení nebo činitele:
   a. Definujete-li uživatele jako alternativního činitele zabezpečení, musí být uživatel stejného uživatele, pod kterým bude spuštěn správce front. Uživatel musí být členem lokální skupiny mqm .
   b. Definujete-li lokální skupinu jako alternativní skupinu zabezpečení, přidejte uživatele, pod kterým bude správce front spuštěn, do alternativní skupiny. Uživatel musí být také členem lokální skupiny mqm .
   c. Definujete-li globální skupinu jako alternativní skupinu zabezpečení, viz “Zabezpečení dat správce sdílených front a adresářů protokolů a souborů v systému Windows” na stránce 487.
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 průvodce "Připravit IBM MQ " . Pro tuto úlohu nakonfigurujte instalaci tak, aby byla spuštěna buď s ID lokálního uživatele, nebo s ID uživatele domény. Nakonec, chcete-li dokončit všechny úlohy v produktu “Windows domén a správců front s více instancemi” na stránce 461, musí být instalace nakonfigurována pro doménu.
3. Chcete-li provést první část úlohy, přihlaste se s oprávněním administrátora.

Informace o této úloze

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 461.

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

“Windows domén a správců front s více instancemi” na stránce 461
Správce front s více instancemi v produktu Windows vyžaduje, aby byla sdílena data a protokoly. Sdílení musí být přístupné pro všechny instance správce front spuštěných na různých serverech nebo pracovních stanicích. Konfigurujte správce front a sdílejte jej jako součást domény produktu Windows . Správce front může být spuštěn na pracovní stanici nebo na serveru domén nebo na řadiči domény.

Související úlohy

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, které jsou autorizovány alternativní globální skupinou zabezpečení” na stránce 474
“Vytvoření správce front s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462

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 průvodce "Připravit IBM MQ " . Pro tuto úlohu nakonfigurujte instalaci tak, aby byla spuštěna buď s ID lokálního uživatele, nebo s ID uživatele domény. Nakonec, chcete-li dokončit všechny úlohy v produktu “Windows domén a správců front s více instancemi” na stránce 461, musí být instalace nakonfigurována pro doménu.
3. Chcete-li provést první část úlohy, přihlaste se s oprávněním administrátora.

Informace o této úloze

Tato úloha je jednou ze sad souvisejících úloh, které ilustrují přístup k datům správce front a souborům protokolu. Tyto úlohy ukazují, jak vytvořit správce front autorizovaného pro čtení a zápis dat a souborů protokolu, které jsou uloženy v adresáři podle vaší volby. Doprovázejí úlohu “Windows domén a správců front s více instancemi” na stránce 461.

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 s více instancemi na pracovních stanicích domény nebo serverech v systému Windows” na stránce 462, ID uživatelů domény vytvořená v “Vytvoření Active Directory a domény DNS v systému Windows” na stránce 465 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 s více instancemi v systému Linux*
Příklad ukazuje, jak nastavit správce front s více instancemi na serveru Linux. Nastavení je malé pro ilustraci zúčastněných pojmů. Tento příklad je založen na systému Linux Red Hat Enterprise 5. Kroky se liší na jiných platformách UNIX .

Informace o této úloze

Příklad je nastaven na 2GHz notebooku se 3 GB RAM spuštěním Windows 7 Service Pack 1. Dva virtuální počítače VMware , Server1 a Server2, spustí Linux Red Hat Enterprise 5 ve snímcích 640 MB. Server Server1 je hostitelem síťového systému souborů (NFS), protokolů správce front a instance HA. Není obvyklé, aby se server NFS také hostili jedné z instancí správce front; to je zjednodušení příkladu. Server Server2 připojí protokoly správce front serveru Server1k instanci v pohotovostním režimu. Klient WebSphere MQ MQI se instaluje na další obraz 400 MB VMware , který spouští produkt Windows 7 Service Pack 1 a spouští ukázkové aplikace s vysokou dostupností. Všechny virtuální počítače jsou konfigurovány jako součást sítě hostitele VMware , a to z důvodů zabezpečení.

Poznámka: Měli byste umístit pouze data správce front na server NFS . Na systému NFSpoužijte k zajištění zabezpečení systému následující tři volby s příkazem mount:

- **neexec**
  Pomocí této volby zabráníte spuštění binárních souborů na systému NFS, což zabrání vzdálenému uživateli v spuštění nežádoucího kódu v systému.

- **nosuid**
  Pomocí této volby zabráníte použití bitů set-user-identifier a set-group-identifier, což zabrání vzdálenému uživateli získat vyšší oprávnění.
- **nodev**
  Pomocí této volby zastavíte používání nebo definování speciálních zařízení nebo blokových speciálních zařízení, která zabrání vzdálenému uživateli dostat se z vězení chroot.

Postup

1. Přihlaste se jako uživatel root.
2. Přečtěte si téma Instalace produktu IBM MQ -přehled a postupujte podle příslušného odkazu k instalaci produktu IBM MQ, vytvoření uživatele a skupiny mqm a definování produktu `/var/mqm`.
3. Dokončete úlohu Ověření chování sdíleného systému souborů a zkontrolujte, zda systém souborů podporuje správce front s více instancemi.
4. Pro Server1dokončete následující krok:
   a. Vytvořte protokol a datové adresáře ve společné složce `/MQHA`, která má být sdílena. Příklad:
      i) **mkdir** */MQHA*
      ii) **mkdir** */MQHA/logs*
      iii) **mkdir** */MQHA/qmgrs*
5. Pro Server2dokončete následující krok:
   a. Vytvořte složku, `/MQHA`, chcete-li připojit sdílený systém souborů. Uchovat cestu stejně jako na serveru Server1. Příklad:
      i) **mkdir** */MQHA*
6. Ujistěte se, že adresáře `MQHA` jsou vlastněny uživatelem a skupinou mqm, a přístupová oprávnění jsou nastavena na `rwx` pro uživatele a skupinu. Například **ls -al** zobrazí `drwxrwxr-x mqm mqm 4096 Nov 27 14:38 MQDATA .`
   a. **chown -R** `mqm:mqm` */MQHA*
   b. **chmod -R** `ug+rwx` */MQHA*
7. Vytvořte správce front zadáním následujícího příkazu: **crtmqm -ld** */MQHA/logs* **-md** */MQHA/qmgrs QM1*
8. Přičíst[2] `/MQHA *(rw,sync,no_wdelay,fsid=0)` na `/etc/exports`
9. Pro server Server1proveďte následující kroky:
   a. Spusťte démona NFS : */etc/init.d/* **nfs** `start`
   b. Zkopírujte podrobnosti o konfiguraci správce front ze serveru Server1: .

      ```
      dspmqinf -o command QM1
      ```

      a zkopírujte výsledek do schránky:

      ```
      addmqinf -s QueueManager
      -v Name=QM1
      -v Directory=QM1
      -v Prefix=/var/mqm
      -v DataPath=/MQHA/qmgrs/QM1
      ```
10. Pro server Server2proveďte následující kroky:
    a. Připojte exportovaný systém souborů `/MQHA` zadáním následujícího příkazu: **mount -t** `nfs4` **-o** `hard,intr` *Server1:/ /MQHA*

[2] Volba '*' povoluje všechny počítače, které mohou dosáhnout tohoto připojení /MQHA pro čtení/zápis. Omezte přístup na produkční počítač.

b. Vložte konfigurační příkaz správce front do serveru Server2:

```
 addmqinf -s QueueManager
-v Name=QM1
-v Directory=QM1
-v Prefix=/var/mqm
-v DataPath=/MQHA/qmgrs/QM1
```

11. Spusťte instance správce front v jednom pořadí s parametrem **-x** : **strmqm -x** QM1.

    Příkaz používaný ke spuštění instancí správce front musí být zadán ze stejné instalace produktu IBM MQ jako příkaz **addmqinf** . Chcete-li spustit a zastavit správce front z jiné instalace, je třeba nejprve nastavit instalaci přidruženou ke správci front pomocí příkazu **setmqm** . Další informace viz setmqm.

Linux *Ověření správce front s více instancemi v systému Linux*

Chcete-li ověřit konfiguraci správce front s více instancemi, použijte ukázkové programy **amqsghac**, **amqsphac** a **amqsmhac** . Toto téma poskytuje vzorovou konfiguraci pro ověření konfigurace správce front s více instancemi v systému Linux Red Hat Enterprise 5.

Ukázkové programy s vysokou dostupností používají automatické opětovné připojení klienta. Dojde-li k selhání připojeného správce front, klient se pokusí znovu připojit ke správci front ve stejné skupině správců front. Popis ukázek, ukázkových programů vysoké dostupnosti, demonstruje opětovné připojení klienta pomocí správce front s jedinou instancí pro zjednodušení. Chcete-li ověřit konfiguraci správce front s více instancemi, můžete použít stejné ukázky s více správci front pro více instancí.

Příklad používá konfiguraci s více instancemi popsanou v části “Vytvoření správce front s více instancemi v systému Linux” na stránce 499. Použijte konfiguraci k ověření, že správce front s více instancemi se přepne na instanci v pohotovostním režimu. Zastavte správce front pomocí příkazu **endmqm** a použijte volbu -s, switchover, option. Programy klienta se znovu připojí k nové instanci správce front a budou pokračovat v práci s novou instancí po mírném zpoždění.

V tomto příkladu je klient spuštěn na systému Windows 7 Service Pack 1. Systém hostuje dva servery VMware Linux , na kterých běží správce front s více instancemi.

Ověření překonání selhání pomocí produktu IBM MQ Explorer

Před použitím ukázkových aplikací k ověření překonání selhání spusťte program IBM MQ Explorer na každém serveru. Přidejte obě instance správce front do každého průzkumníku pomocí průvodce **Přidat vzdáleného správce front > Připojit přímo k víceinstanceinstanční správci front** . Ujistěte se, že obě instance jsou spuštěny, což umožňuje pohotovostní režim. Zavřete okno se spuštěnou instancí VMware s aktivní instancí, virtuálně vypněte server, nebo zastavte aktivní instanci, což umožňuje přepnutí do rezervní instance.

Poznámka: Pokud vypnete server, ujistěte se, že se nejedná o hostitelský systém /MQHA !

Poznámka: Volba **Povolit přepnutí na instanci v pohotovostním režimu** nemusí být k dispozici v dialogovém okně **Zastavit správce front** . Volba chybí, protože správce front je spuštěn jako správce front s jednou instancí. Musíte je spustit bez volby **Povolit instanci v pohotovostním režimu** . Pokud je váš požadavek na zastavení správce front odmítnut, podívejte se do okna **Podrobnosti** , je to možné, protože neexistuje žádná instance v pohotovostním režimu.

Ověření překonání selhání pomocí ukázkových programů

Vyberte server, na kterém má být spuštěna aktivní instance

Je možné, že jste zvolili jeden ze serverů pro hostování adresáře MQHA nebo systému souborů. Pokud plánujete otestovat překonání selhání zavřením okna VMware se spuštěným aktivním serverem, ujistěte se, že to není ten, který hostuje MQHA !

Na serveru, na kterém je spuštěna aktivní instance správce front

Poznámka: Spuštění kanálu produktu SVRCONN s parametrem MCAUSER nastaveným na hodnotu mqmje výhodné snížit počet kroků konfigurace uvedených v příkladu. Je-li zvoleno jiné ID uživatele a váš systém je nastaven jinak než ten, který se používá v příkladu, můžete se setkat

s problémy s přístupovým oprávněním. Nepoužívejte mqm jako MCAUSER na vystaveném systému; je pravděpodobné, že se výrazně ohrozí bezpečnostní riziko.

1. Upravte hodnoty *ipaddr1* a *ipaddr2* a uložte následující příkazy v produktu /MQHA/ hasamples.tst. .

```
DEFINE QLOCAL(SOURCE) REPLACE
DEFINE QLOCAL(TARGET) REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(SVRCONN)  TRPTYPE(TCP) +
MCAUSER('mqm') REPLACE
DEFINE CHANNEL(CHANNEL1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) +
CONNAME(' ipaddr1 (1414), ipaddr2
(1414)') QMNAME(QM1) REPLACE
START  CHANNEL(CHANNEL1)
DEFINE LISTENER(LISTENER.TCP) TRPTYPE(TCP) CONTROL(QMGR)
DISPLAY LISTENER(LISTENER.TCP) CONTROL
START  LISTENER(LISTENER.TCP)
DISPLAY LSSTATUS(LISTENER.TCP) STATUS
```

2. Otevřete okno terminálu s cestou /MQHA a spusťte příkaz:

```
runmqsc -m QM1 < hasamples.tst
```

3. Ověřte, zda je modul listener spuštěný a má-li řízení správce front, a to buď kontrolou výstupu příkazu **runmqsc** .

```
LISTENER(LISTENER.TCP)CONTROL(QMGR)
LISTENER(LISTENER.TCP)STATUS(RUNNING)
```

   Nebo pomocí IBM MQ Explorer , který spouští modul listener protokolu TCP/IP, a má Control = Queue Manager.

Na klientu

1. Zkopírujte tabulku připojení klienta AMQCLCHL.TAB z /MQHA/qmgrs/QM1.000/@ipcc na serveru na C:\ na klientovi.
2. Otevřete příkazový řádek s cestou C:\ a nastavte proměnnou prostředí MQCHLLIB tak, aby ukazovala na tabulku definic kanálů klienta (CCDT).

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

3. Na příkazový řádek zadejte příkazy:

```
start amqsghac TARGET QM1
start amqsmhac -s SOURCE -t TARGET -m QM1
start amqsphac SOURCE QM1
```

Na serveru, na kterém je spuštěna aktivní instance správce front

1. Proveďte jednu z následujících akcí:
   - Zavřete okno se spuštěnou instancí serveru VMware s obrazem aktivního serveru.
   - Pomocí konzoly IBM MQ Explorerzastavte aktivní instanci správce front, což umožňuje přepnutí na záložní instanci a instruování opakovaného připojení klientů k opětovnému připojení.
2. Tři klienti nakonec zjistí, že spojení je přerušeno, a pak se znovu připojí. V této konfiguraci, pokud zavřete okno serveru, trvá přibližně sedm minut, než se znovu ustanoví všechna tři připojení. Některá spojení se znovu ustanoví dobře před ostatními.

Výsledky

```
N:\>amqsphac SOURCE QM1
Sample AMQSPHAC start
target queue is SOURCE
message Message 1
message Message 2
message Message 3
message Message 4
message Message 5
17:05:25 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:47 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:52 : EVENT : Connection Reconnected
message Message 6
message Message 7
message Message 8
message Message 9
```

```
N:\>amqsmhac -s SOURCE -t TARGET -m QM1
Sample AMQSMHA0 start

17:05:25 : EVENT : Connection Reconnecting (Delay: 97ms)
17:05:48 : EVENT : Connection Reconnecting (Delay: 0ms)
17:05:53 : EVENT : Connection Reconnected
```

```
N:\>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 víceinstanční správce front zcela odstranit, použijte příkaz **dltmqm** k odstranění správce front a potom odeberte instance z jiných serverů pomocí příkazů **rmvmqinf** nebo **dltmqm** .

Spuštěním příkazu **dltmqm** odstraňte správce front s instancemi, které jsou definovány na jiných serverech, na libovolném serveru, na kterém je správce front definován. Není třeba spouštět příkaz **dltmqm** na stejném serveru, na kterém jste jej vytvořili. Poté spusťte příkaz **rmvmqinf** nebo **dltmqm** na všech ostatních serverech, které mají definici správce front.

Správce front můžete odstranit pouze v případě, že je zastaven. Ve chvíli, kdy jej odstraníte, nejsou spuštěny žádné instance a správce front striktně řečeno není ani jedním nebo více správcem front pro více instancí; je to jednoduše správce front, který má svá data správce front a protokoly na vzdáleném sdílení. Při odstranění správce front dojde k odstranění jeho dat a protokolů správce front a ze souboru `mqs.ini` na serveru, na kterém jste zadali příkaz **dltmqm** , je odebrán oddíl správce front. Při odstraňování správce front je třeba mít přístup ke sdílenému síťovému sdílení, které obsahuje data správce front a protokoly.

Na jiných serverech, na kterých jste dříve vytvořili instance správce front, jsou na těchto serverech také položky v souborech `mqs.ini` . Je třeba navštívit každý server a odstranit sekci správce front spuštěním příkazu **rmvmqinf** *název oddílu správce front*.

Linux UNIX Pokud jste v systémech UNIX and Linux umístili společný soubor `mqs.ini` do síťového úložiště a odkazovali na něj ze všech serverů nastavením proměnné prostředí `AMQ_MQS_INI_LOCATION` na každém serveru, pak musíte správce front odstranit pouze z jednoho ze svých serverů, protože je k dispozici pouze jeden soubor `mqs.ini` .

Příklad

První server

dltmqm QM1

Další servery, kde jsou definovány instance

rmvmqinf QM1 nebo

dltmqm QM1

Multi *Spuštění a zastavení správce front s více instancemi*

Spuštění a zastavení správce front konfigurovaného na více platformách jako jedna instance nebo správce front s více instancemi.

Pokud jste definovali správce front s více instancemi na dvojici serverů, můžete správce front spustit na obou serverech buď jako správce front s jednou instancí, nebo jako správce front s více instancemi.

Chcete-li spustit správce front s více instancemi, spusťte správce front na jednom ze serverů s použitím příkazu **strmqm** -x *QM1* ; volba -x povoluje instanci pro překonání selhání. Stane se *aktivní instancí*. Spusťte rezervní instanci na druhém serveru pomocí stejného příkazu **strmqm** -x *QM1* ; volba -x povoluje, aby se instance spustila jako rezervní.

Správce front je nyní spuštěn s jednou aktivní instancí, která zpracovává všechny požadavky, a záložní instanci, která je připravena převzít, pokud dojde k selhání aktivní instance. Aktivní instance má udělen výlučný přístup k datům a protokolům správce front. Záložní server čeká na udělení výlučného přístupu k datům a protokolům správce front. Je-li do rezervní databáze udělen výlučný přístup, stane se aktivní instancí.

Můžete také ručně přepnout řízení na rezervní instanci zadáním příkazu **endmqm** -s na aktivní instanci. Příkaz **endmqm** -s ukončí běh aktivní instance bez ukončení činnosti pohotovostního režimu. Zámek výlučného přístupu k datům a protokolům správce front je uvolněn a rezervní databáze převezme funkci.

Můžete také spustit a zastavit správce front, který je konfigurován s více instancemi na různých serverech, jako správce front s jednou instancí. Pokud správce front spustíte bez použití volby -x u příkazu **strmqm** , nebude možné spouštět instance správce front konfigurovaného v jiných počítačích jako instance v pohotovostním režimu. Pokusíte-li se spustit jinou instanci, obdržíte odezvu, že instance správce front není povolena ke spuštění jako rezervní databáze.

Zastavíte-li aktivní instanci správce front s více instancemi pomocí příkazu **endmqm** bez volby -s , budou aktivní i rezervní instance zastaveny. Pokud zastavíte instanci v pohotovostním režimu pomocí příkazu **endmqm** s volbou -x , zastaví se jako záložní a aktivní instance bude pokračovat v činnosti. Nemůžete vydat příkaz **endmqm** bez volby -x v pohotovostním režimu.

Ve stejnou dobu mohou být spuštěny pouze dvě instance správce front; jedna z nich je aktivní instance a druhá instance je rezervní instance. Pokud spustíte dvě instance současně, produkt IBM MQ nemá žádnou kontrolu nad tím, který instance se stane aktivní instancí; je určen síťovým systémem souborů. První instance, která má získat výhradní přístup k datům správce front, se stane aktivní instancí.

Poznámka: Před restartováním správce front, který selhal, je třeba odpojit vaše aplikace od této instance správce front. Pokud tomu tak není, nemusí se správce front restartovat správně.

Multi *Sdílený systém souborů*

Na platformě Mulitplatforms používá správce front s více instancemi síťovému systému souborů ke správě instancí správce front.

Správce front s více instancemi automatizuje překonání selhání pomocí kombinace zámků systému souborů a sdílených dat správce front a protokolů. Pouze jedna instance správce front může mít výlučný

přístup k datům a protokolům sdíleného správce front. Když se získá přístup, stane se aktivní instancí. Druhá instance, která nemá úspěch při získávání výlučného přístupu, bude čekat jako záložní instance, dokud nebudou zpřístupněna data a data správce front.

Systém souborů připojený k síti je odpovědný za uvolnění zámků, které ukládá pro aktivní instanci správce front. Pokud aktivní instance selže nějakým způsobem, síťový systém souborů uvolní zámky, které zadržuje pro aktivní instanci. Jakmile je uvolněn výlučný zámek, čeká se záložní správce front, který čeká na získání zámku. Pokud uspěje, stane se aktivním instancí a má výlučný přístup k datům a protokolům správce front v rámci sdíleného systému souborů. Poté se pokračuje ve spouštění.

Související téma Plánování podpory systému souborů popisuje, jak lze nastavit a zkontrolovat, zda váš systém souborů podporuje správce front s více instancemi.

Správce front s více instancemi vás neochrání před selháním v systému souborů. Existuje celá řada způsobů, jak chránit vaše data.

- Investujte do spolehlivého úložiště, jako je pole RAID (redundant disk array), a zahrňte je do síťového systému souborů, který má odolnost sítě.
- Zazálohujte lineární protokoly IBM MQ na alternativní média, a pokud se médium primárního protokolu nezdaří, proveďte obnovu pomocí protokolů na alternativním médiu. Ke správě tohoto procesu můžete použít správce front zálohování.

Multi *Více instancí správce front*

Správce front s více instancemi je odolný, protože používá pohotovostní instanci správce front k obnovení dostupnosti správce front po selhání.

Replikace instancí správce front je velmi účinným způsobem pro zlepšení dostupnosti procesů správce front. Použití jednoduchého modelu dostupnosti, pouze pro ilustraci: je-li spolehlivost jedné instance správce front 99% (více než jeden rok, kumulativní výpadek je 3.65 dní), pak přidání další instance správce front zvýší dostupnost na 99.99% (více než jeden rok, kumulativní výpadek přibližně za hodinu).

Tento model je příliš jednoduchý na to, aby vám poskytl praktické numerické odhady dostupnosti. Chcete-li modelovat dostupnost realisticky, musíte sbírat statistiku pro střední dobu mezi poruchami (MTBF) a průměrnou dobu na opravu (MTTR) a pravděpodobnostní rozdělení času mezi poruchami a časy oprav.

Termín správce front s více instancemi odkazuje na kombinaci aktivních a rezervních instancí správce front, které sdílejí data a protokoly správce front. Správci front s více instancemi vás ochrání před selháním procesů správce front tím, že budou mít jednu instanci správce front aktivní na jednom serveru, a další instanci správce front v pohotovostním režimu na jiném serveru, která je připravena k převzetí automaticky, pokud dojde k selhání aktivní instance.

Multi *Přepnutí nebo přepnutí*

Instance správce front v pohotovostním režimu přebírá z aktivní instance buď na požadavek (přepnutí), nebo když dojde k selhání aktivní instance (přepnutí při selhání).

- *Přepnutí* se provede tehdy, když se instance rezervní databáze spustí jako odpověď na příkaz **endmqm** `-s` , který je vydán do aktivní instance správce front. Můžete určit parametry **endmqm** `-c`, `-i` nebo `-p` , které určují, jak je správce front náhle ukončen.

  Poznámka: Přepnutí se provede pouze v případě, že je instance správce front v pohotovostním režimu již spuštěna. Příkaz **endmqm** `-s` uvolní zámek aktivního správce front a povolí přepnutí: nespustí instanci správce front v pohotovostním režimu.
- *Překonání selhání* nastane, když je zámek na datech správce front v držení aktivní instance uvolněn, protože se neočekávaně zastavil instance (tj. bez zadání příkazu **endmqm**).

Když se záložní instance převezme jako aktivní instance, zapíše zprávu do protokolu chyb správce front.

Reconnetable klienti jsou automaticky znovu připojeni, když selže správce front nebo se přepíná. Chcete-li požadovat opětovné připojení klienta, nemusíte do příkazu **endmqm** zahrnout příznak `-r` . Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Pokud zjistíte, že nelze restartovat selhání instance, i když došlo k překonání selhání a záložní instance se stala aktivní, zkontrolujte, zda se aplikace připojené lokálně k instanci, která selhala, odpojovaly od nezdařené instance.

Lokálně připojené aplikace musí skončit nebo se odpojit od nezdařené instance správce front, aby se instance, která selhala, restartovala. Všechny lokálně připojené aplikace používající sdílené vazby (což je výchozí nastavení), které se drží připojení k nezdařeným instancím instance, aby se zabránilo restartování instance.

Pokud není možné ukončit lokálně připojené aplikace, nebo zajistit, aby se odpojily při selhání lokální instance správce front, zvažte použití izolovaných vazeb. Lokálně připojené aplikace používající izolované vazby nezabrání restartování lokální instance správce front, a to i v případě, že se neodpojí.

Multi *Připojení kanálu a klienta znovu*

Připojení kanálu a klienta je nezbytnou součástí obnovení zpracování zpráv po aktivaci instance správce front v pohotovostním režimu.

Instance správce front s více instancemi jsou instalovány na serverech s různými síťovými adresami. Je třeba nakonfigurovat kanály a kanály produktu IBM MQ s informacemi o připojení pro všechny instance správce front. Když se záloha převezme, klienti a kanály jsou automaticky znovu připojeni k nově aktivní instanci správce front na nové síťové adrese. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Návrh se liší od způsobu práce s vysokou dostupností, jako jsou například práce typu HA-CMP. Objekt HA-CMP poskytuje virtuální adresu IP pro klastr a přenáší adresu k aktivnímu serveru. IBM MQ opětovné připojení nemění nebo přesměrovávat adresy IP. Pracuje tak, že se znovu propojí s použitím síťových adres, které jste definovali v definicích kanálů a připojeních klientů. Jako administrátor musíte definovat síťové adresy v definicích kanálů a připojení klienta ke všem instancím libovolného správce front s více instancemi. Nejlepší způsob konfigurace síťových adres pro správce front s více instancemi závisí na připojení:

Kanály správce front
Atribut CONNAME kanálů je čárkami oddělený seznam názvů připojení; například `CONNAME('127.0.0.1(1234), 192.0.2.0(4321)')`. Připojení se zkoušejí v pořadí uvedeném v seznamu připojení, dokud nebude úspěšně ustanoveno připojení. Není-li připojení úspěšné, kanál se pokusí znovu připojit.

Kanály klastru

Obvykle není zapotřebí žádná další konfigurace pro vytvoření správců front s více instancemi v klastru.

Pokud se správce front připojí ke správci front úložiště, zjistí úložiště síťovou adresu správce front. Tento parametr odkazuje na CONNAME kanálu produktu CLUSRCVR na správci front. Při použití protokolu TCPIP správce front automaticky nastaví parametr CONNAME , pokud jej vynecháte, nebo jej konfigurujte na prázdné místo. Když se převezme rezervní instance, jeho adresa IP nahradí adresu IP předchozí aktivní instance jako CONNAME.

Je-li to nezbytné, můžete ručně nakonfigurovat CONNAME se seznamem síťových adres instancí správce front.

Připojení klienta
Připojení klienta mohou používat seznamy připojení nebo skupiny správců front k výběru alternativních připojení. Je třeba, aby klienti byli kompilovány ke spuštění s klientskými knihovnami klienta IBM WebSphere MQ 7.0.1 nebo lepší. Musí být připojeny alespoň ke správci front produktu IBM WebSphere MQ 7.0.1 .

Když dojde k překonání selhání, opětovné připojení zabere nějaký čas. Záložní správce front musí dokončit spuštění. Klienti, kteří byli připojeni k selhání správce front, musí zjistit selhání připojení a spustit nové připojení klienta. Pokud nové připojení klienta vybere rezervní správce front, který se stal nově aktivním, je klient znovu připojen ke stejnému správci front.

Je-li klient v polovině volání MQI během opětovného připojení, musí před dokončením volání tolerovat delší čekání.

Pokud dojde k selhání během dávkového přenosu na kanálu zpráv, dávka se vrátí zpět a restartuje.

Přepnutí je rychlejší než přestavení a trvá pouze tak dlouho, jako je zastavování jedné instance správce front a spuštění druhé. Pro správce front s pouhými několika záznamy protokolu k přehrání může v nejlepším přepnutí trvat několik sekund. Chcete-li odhadnout, jak dlouho trvá překonání selhání, musíte přidat čas, který trvá, než bude detekováno selhání. Nejlepší detekce trvá 10 sekund a může to trvat několik minut, v závislosti na síti a systému souborů.

Multi *Obnova aplikace*

Obnova aplikací je automatické pokračování zpracování aplikací po překonání selhání. Obnova aplikace po překonání selhání vyžaduje důkladný návrh. Některé aplikace vyžadují, aby došlo k překonání selhání.

Cílem obnovy aplikace je, aby aplikace pokračovala ve zpracování pouze s krátkou prodlevou. Než budete pokračovat v novém zpracování, aplikace se musí vrátit zpět a znovu odeslat pracovní jednotku, kterou zpracovával během selhání.

Problém při zotavení aplikace ztrácí kontext, který je sdílen mezi produktem IBM MQ MQI client a správcem front a který je uložen ve správci front. IBM MQ MQI client obnovuje většinu kontextu, ale existují některé části kontextu, které nelze spolehlivě obnovit. V následujících částech jsou popsány některé vlastnosti obnovy aplikací a informace o tom, jak ovlivňují zotavení aplikací připojených ke správci front s více instancemi.

Transakční systém zpráv

Z pohledu doručování zpráv nemění překonání selhání trvalé vlastnosti systému zpráv produktu IBM MQ . Pokud jsou zprávy trvalé a jsou správně spravovány v rámci jednotek práce, zprávy se během překonání selhání neztratí.

Z pohledu zpracování transakcí jsou transakce buď zálohovány nebo potvrzeny po překonání selhání.

Nepotvrzené transakce jsou odvolány. Po překonání selhání obdrží znovu připojitelná aplikace `MQRC_BACKED_OUT` kód příčiny, aby označoval, že transakce se nezdařila. Poté musí transakci znovu spustit znovu.

Potvrzené transakce jsou transakce, které dosáhly druhé fáze dvoufázového potvrzovacího procesu nebo transakce s jednou fází (pouze zprávy), které začaly `MQCMIT`.

Je-li správce front koordinátorem transakce a `MQCMIT` zahájil druhou fázi své dvoufázové operace commit před selháním, transakce se úspěšně dokončí. Dokončení je pod kontrolou správce front a bude pokračovat, když je správce front spuštěn znovu. V repřipojitelné aplikaci je volání `MQCMIT` normálně dokončeno.

V jednofázovém potvrzení, které zahrnuje pouze zprávy, je transakce, která zahájila zpracování potvrzení, za normálních okolností pod kontrolou správce front, jakmile je spuštěna znovu. V repřipojitelné aplikaci se `MQCMIT` dokončí normálně.

Znovu připojitelné klienti mohou používat transakce s jednoduchou fází pod kontrolou správce front jako koordinátor transakcí. Rozšířený transakční klient nepodporuje opětovné připojení. Je-li požadováno opětovné připojení, když se připojuje transakční klient, připojení bude úspěšné, ale bez možnosti opětovného připojení. Připojení se chová, jako by se nepřipojitelné k tabulce.

Restart aplikace nebo pokračování

Překonání selhání přeruší aplikaci. Po selhání se může aplikace restartovat od začátku, nebo může pokračovat ve zpracování po přerušení. Tento příkaz se nazývá *automatické opětovné připojení klienta*. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Pomocí aplikace IBM MQ MQI client můžete nastavit volbu připojení pro automatické opětovné připojení klienta. Volby jsou `MQCNO_RECONNECT` nebo `MQCNO_RECONNECT_Q_MGR`. Není-li nastavena žádná volba, klient se nepokusí znovu připojit automaticky a selhání správce front se vrátí klientovi `MQRC_CONNECTION_BROKEN` . Můžete navrhnout klienta, abyste se pokusili spustit nové připojení zadáním nového volání `MQCONN` nebo `MQCONNX` .

Programy serveru je třeba restartovat; správce front nemůže automaticky znovu připojit, a to v okamžiku, kdy došlo k selhání správce front nebo serveru. Programy serveru IBM MQ se při selhání instance správce front s více instancemi zpravidla nerestartuje na instanci správce front v pohotovostním režimu.

Program na serveru IBM MQ můžete automatizovat, aby se restartoval na záložním serveru dvěma způsoby:

1. Zabalte aplikaci serveru jako službu správce front. Restartuje se, když se správce front v pohotovostním režimu restartuje.
2. Zadejte vlastní logiku pro překonání selhání, která se spustí například při spuštění zprávy protokolu o překonání selhání, kterou zapsal záložní instance správce front. Instance aplikace pak musí po spuštění volat MQCONN nebo MQCONNX , aby bylo možné vytvořit připojení ke správci front.

Detekce překonání selhání

Některé aplikace si musí být vědomi překonání selhání, jiné nikoli. Zvažte tyto dva příklady.

1. Aplikace systému zpráv, která přijímá nebo přijímá zprávy prostřednictvím kanálu systému zpráv, standardně nevyžaduje spuštění správce front na druhém konci kanálu: pravděpodobně nebude ovlivněn, pokud správce front na druhém konci kanálu restartuje v rámci instance v pohotovostním režimu.
2. Aplikace IBM MQ MQI client zpracovává trvalý vstup zpráv z jedné fronty a ukládá trvalé odpovědi na zprávy do jiné fronty jako součást jediné transakce: pokud zpracovává kód příčiny MQRC_BACKED_OUT z MQPUT, MQGET nebo MQCMIT v rámci synchronizačního bodu restartováním pracovní jednotky, pak se neztratí žádné zprávy. Aplikace navíc nemusí provádět žádné speciální zpracování při pokusu o navázání spojení se selháním připojení.

Předpokládejme však, že v druhém příkladu je aplikace prohledáváním fronty a výběru zprávy ke zpracování pomocí volby MQGET , MQGMO_MSG_UNDER_CURSOR. Reconnction resetuje kurzor procházení a volání MQGET nevrátí správnou zprávu. V tomto příkladu se vyskytla aplikace, která má být informovaná o překonání selhání. Kromě toho musí před vydáním jiného příkazu MQGET pro zprávu pod kurzorem aplikace obnovit kurzor procházení.

Ztráta kurzoru při procházení představuje jeden příklad, jak se mění kontext aplikace po opětovném připojení. Další případy jsou dokumentovány v příručce “Zotavení automaticky znovu připojeného klienta” na stránce 509.

Máte tři alternativní vzory návrhu pro aplikace produktu IBM MQ MQI client po překonání selhání. Pouze jeden z nich není třeba detekovat překonání selhání.

Bez opětovného připojení

V tomto vzorku zastaví aplikace veškeré zpracování aktuálního připojení, jakmile dojde k přerušení spojení. Má-li aplikace pokračovat ve zpracování, musí vytvořit nové připojení ke správci front. Aplikace je zcela odpovědná za přenos všech informací o stavu, které vyžaduje, aby pokračovalo zpracování na novém připojení. Existující klientské aplikace, které se znovu připojí ke správci front po ztrátě spojení, jsou tímto způsobem zapsány.

Klient obdrží kód příčiny, například MQRC_CONNECTION_BROKENnebo MQRC_Q_MGR_NOT_AVAILABLE , z dalšího volání MQI po ztrátě spojení. Aplikace musí vyřadit všechny své informace o stavu IBM MQ , jako jsou popisovače fronty, a vydat nové volání MQCONN nebo MQCONNX k vytvoření nového připojení a poté znovu otevřít objekty produktu IBM MQ , které potřebuje ke zpracování.

Výchozí chování MQI je pro popisovač připojení ke správci front, který má být nepoužitelný po ztrátě připojení ke správci front. Předvolba je ekvivalentní nastavení volby MQCNO_RECONNECT_DISABLED v systému MQCONNX , aby se zabránilo opětovnému připojení aplikace po překonání selhání.

Překonání selhání

Zapište aplikaci tak, aby nebyla ovlivněna překonáním selhání. Někdy je třeba pečlivě sledovat ošetřování chyb při řešení překonání selhání.

Reconnuction aware
Zaregistrujte obslužnou rutinu událostí MQCBT_EVENT_HANLER se správcem front. Obslužná rutina událostí se uveřejní v produktu MQRC_RECONNECTING , když se klient spustí při pokusu o opětovné připojení k serveru a MQRC_RECONNECTED po úspěšném opětovném připojení. Poté můžete spustit rutinu tak, aby znovu vytvořila předvídatelný stav, takže klientská aplikace bude schopna pokračovat ve zpracování.

Zotavení automaticky znovu připojeného klienta

Překonání selhání je neočekávaná událost a pro automaticky připojovaného klienta k práci, jak je navrženo důsledky opětovného připojení, musí být předvídatelné.

Hlavním prvkem obratu neočekávaného selhání v předvídatelném a spolehlivém zotavení je použití transakcí.

V předchozí sekci byl zadán příklad “2” na stránce 508, který byl zadán IBM MQ MQI client pomocí lokální transakce pro koordinaci MQGET a MQPUT. Klient vydá chybu MQCMIT nebo MQBACK v odezvě na chybu MQRC_BACKED_OUT a poté znovu odešle zálohovanou transakci. Selhání správce front způsobí, že transakce bude vrácena a chování aplikace klienta zajistí, že nebudou ztraceny žádné transakce a žádné zprávy.

Ne všechny programové stavy jsou spravovány jako součást transakce, a proto je obtížné porozumět následkům opětovného připojení. Musíte vědět, jak opětovné připojení změní stav IBM MQ MQI client , aby bylo možné navrhnout aplikaci klienta, aby přežila překonání selhání správce front.

Můžete se rozhodnout navrhnout svou aplikaci bez speciálního kódu pro překonání selhání a s jinými chybami znovu zacházet s chybami opětovného připojení se stejnou logikou. Případně můžete zvolit, že opětovné připojení vyžaduje speciální zpracování chyb, a zaregistrujte obslužnou rutinu událostí s produktem IBM MQ ke spuštění rutiny pro překonání selhání. Rutina může pracovat se zpracováním opětovného připojení nebo nastavit příznak tak, aby indikoval vláknu hlavního programu, že když bude pokračovat ve zpracování, je třeba provést zpracování zotavení.

Prostředí IBM MQ MQI client si je vědomo samotné překonání selhání a obnovuje se tak, jak může, po opětovném připojení, uložením některých informací o stavu v klientovi a vydáním dalších volání MQI v zastoupení klientské aplikace za účelem obnovení stavu IBM MQ . Například jsou obnoveny objekty, které byly otevřené v bodu selhání, a dočasné dynamické fronty se otevírají se stejným názvem. Existují však změny, které jsou nevyhnutelné a vy potřebujete váš návrh na vypořádání se s těmito změnami. Změny lze rozdělit do pěti druhů:

1. Nová nebo dříve nediagnostikovaná chyba se vrací z volání MQI, dokud aplikační program neobnoví konzistentní nový stav kontextu.

   Příklad přijetí nové chyby je návratový kód MQRC_CONTEXT_NOT_AVAILABLE při pokusu o předání kontextu po uložení kontextu před opětovným připojením. Kontext nelze obnovit po novém připojení, protože kontext zabezpečení nebyl předán neautorizovanému programu klienta. Chcete-li tak učinit, aby mohl škodlivý aplikační program získat kontext zabezpečení.

   Obvykle aplikace zpracovávají běžné a předvídatelné chyby v pečlivě navrženým způsobem a relegují méně časté chyby na generickou obslužnou rutinu chyb. Obslužná rutina chyb se může odpojit od IBM MQ a znovu se znovu připojit, nebo dokonce zastavit program úplně. Chcete-li zlepšit kontinuitu, je možné, že se budete muset vypořádat s některými chybami jinak.
2. Netrvalé zprávy mohou být ztraceny.
3. Transakce jsou odvolány.
4. Volání MQGET nebo MQPUT použitá mimo bod synchronizace mohou být přerušeny s možnou ztrátou zprávy.
5. Při dlouhodobém čekání na volání MQI došlo k chybám způsobeným načasným načasným načasným čekáním.

Některé podrobnosti o ztrátě kontextu jsou uvedeny v následující sekci.

- Netrvalé zprávy jsou vyřazeny, pokud nebyly vloženy do fronty s volbou NPMCLASS (HIGH) a selhání správce front nepřeruší volbu ukládání přechodných zpráv při ukončení práce systému.
- Netrvalý odběr je ztracen, je-li přerušeno připojení. Při opětovném připojení se znovu zavádí. Zvažte použití trvalého odběru.
- Interval get-wait se přepočítá; pokud je překročen jeho limit, vrátí hodnotu MQRC_NO_MSG_AVAILABLE. Podobně se znovu vypočítá vypršení platnosti odběru tak, aby poskytly stejnou celkovou dobu vypršení platnosti.
- Pozice kurzoru pro procházení ve frontě je ztracena; je obvykle znovu vytvořena před první zprávou.
  - Volání MQGET , která uvádí MQGMO_BROWS_MSG_UNDER_CURSOR nebo MQGMO_MSG_UNDER_CURSOR, se nezdaří s kódem příčiny MQRC_NO_MSG_AVAILABLE.
  - Zprávy zamknuté pro procházení jsou odemčeny.
  - Procházet označené zprávy s rozsahem platnosti popisovače jsou neoznačené a lze je znovu procházet.
  - Ve většině případů jsou označené zprávy ve většině případů neoznačené.
- Kontext zabezpečení je ztracen. Pokusy o použití kontextu uložené zprávy, jako např. vložení zprávy s MQPMO_PASS_ALL_CONTEXT , selžou s produktem MQRC_CONTEXT_NOT_AVAILABLE.
- Tokeny zpráv jsou ztraceny. MQGET používající token zprávy vrátí kód příčiny MQRC_NO_MSG_AVAILABLE.

  Poznámka: *MsgId* a *CorrelId*, protože jsou součástí zprávy, jsou zachovány se zprávou během překonání selhání, a proto MQGET pomocí MsgId nebo CorrelId pracuje podle očekávání.
- Zprávy vkládané do fronty pod bodem synchronizace v nepotvrzené transakci již nejsou k dispozici.
- Zpracování zpráv v logickém pořadí, nebo ve skupině zpráv, má za následek návratový kód MQRC_RECONNECT_INCOMPATIBLE po opětovném připojení.
- Volání MQI může vrátit MQRC_RECONNECT_FAILED spíše než obecnější MQRC_CONNECTION_BROKEN , které klienti obvykle přijímají dnes.
- Opětovné připojení během volání MQPUT mimo synchronizační bod vrátí hodnotu MQRC_CALL_INTERRUPTED , pokud IBM MQ MQI client neví, zda byla zpráva úspěšně doručena správci front. Opětovné připojení během MQCMIT se chová podobně.
- Příkaz MQRC_CALL_INTERRUPTED je vrácen-po úspěšném opětovném připojení-pokud produkt IBM MQ MQI client neobdržel od správce front žádnou odpověď, aby označil úspěch nebo selhání
  - Doručování trvalé zprávy pomocí volání MQPUT mimo synchronizační bod.
  - Doručování trvalé zprávy nebo zprávy s výchozí perzistencí pomocí volání MQPUT1 mimo synchronizační bod.
  - potvrzení transakce pomocí volání MQCMIT. Odezva se vrátí pouze po úspěšném opětovném připojení.
- Kanály jsou restartovány jako nové instance (mohou se také jednat o různé kanály), a proto se nezachová žádný stav ukončení kanálu.
- Dočasné dynamické fronty se obnoví jako část procesu obnovy klientů s možností opětovného připojení, které měly otevřené dočasné dynamické fronty. Žádné zprávy v dočasné dynamické frontě nejsou obnoveny, ale aplikace, které měly frontu otevřenou, nebo si zapamatovali název fronty, jsou schopny pokračovat ve zpracování.

  Je zde možnost, že pokud je fronta používána jinou aplikací, než je ta, která ji vytvořila, nemusí být obnovena dostatečně rychle, aby mohla být přítomna, když se na ni bude příště odkazovat. Pokud například klient vytvoří dočasnou dynamickou frontu jako frontu pro odpovědi na frontu a do fronty bude vložena zpráva s odezvou, nemusí být fronta vrácena včas. V tomto případě by kanál obvykle umístil odpověď-na zprávu do fronty nedoručených zpráv.

  Pokud aplikace klienta s možností opětovného připojení otevře dočasnou dynamickou frontu podle názvu (protože ji již vytvořila jiná aplikace) a poté dojde k opětovnému připojení, produkt IBM MQ MQI client nemůže znovu vytvořit dočasnou dynamickou frontu, protože nemá model, ze kterého by jej

vytvořil. V rozhraní MQI může dočasnou dynamickou frontu v rámci modelu otevřít pouze jedna aplikace. Ostatní aplikace, které chtějí použít dočasnou dynamickou frontu, musí používat vazby MQPUT1nebo vazby serveru nebo mohou znovu zkusit opětovné připojení, pokud se nezdaří.

Do dočasné dynamické fronty mohou být vloženy pouze přechodné zprávy a tyto zprávy se ztratí během překonání selhání. Tato ztráta má hodnotu true pro zprávy, které jsou do dočasné dynamické fronty vloženy pomocí příkazu MQPUT1 během opětovného připojení. Pokud dojde k překonání selhání během operace MQPUT1, nemusí být zpráva vložena, ačkoli je parametr MQPUT1 úspěšný. Alternativním řešením tohoto problému je použití trvalých dynamických front. Každá aplikace pro vázání serveru může otevřít dočasnou dynamickou frontu podle názvu, protože ji nelze znovu připojit.

Multi *Zotavení dat a vysoká dostupnost*

Řešení vysoké dostupnosti s pomocí správců front s více instancemi musí zahrnovat mechanismus k obnovení dat po selhání úložiště.

Správce front s více instancemi zvyšuje dostupnost procesů správce front, nikoli však dostupnost jiných komponent, jako je například systém souborů, který správce front používá k ukládání zpráv a další informace.

Jedním ze způsobů, jak zajistit vysokou dostupnost dat, je použití odolného datového úložiště odolných vůči síti. Můžete buď sestavit své vlastní řešení pomocí síťového systému souborů a odolného datového úložiště, nebo si můžete zakoupit integrované řešení. Chcete-li skloubit odolnost vůči zotavení z havárie, pak je k dispozici asynchronní replikace disku, která umožňuje replikaci disku přes desítky nebo stovky kilometrů.

Můžete nakonfigurovat způsob, jakým jsou mapovány různé adresáře produktu IBM MQ na paměťová média, abyste dosáhli co nejlepšího využití médií. Pro správce front *více instancí* je důležité rozlišovat mezi dvěma typy adresářů a souborů IBM MQ .

Adresáře, které musí být sdíleny mezi instancemi správce front.
Informace, které musí být sdíleny mezi různými instancemi správce front, se nacházejí ve dvou adresářích: z adresářů `qmgrs` a `logs` . Adresáře musí být na sdíleném síťovém systému souborů. Doporučuje se používat paměťová média, která poskytuje nepřetržitou vysokou dostupnost a vynikající výkon, protože data se neustále mění v podobě zpráv, které jsou vytvářeny a odstraňovány.

Adresáře a soubory, které nemají *mají* být sdíleny mezi instancemi správce front.
Některé jiné adresáře nemusí být sdíleny mezi různými instancemi správce front a jsou rychle obnoveny jiným způsobem než pomocí zrcadlového systému souborů.

- Spustitelné soubory IBM MQ a adresář nástrojů. Nahraďte opětovnou instalací nebo zálohováním a obnovením z archivu zálohovaného souboru.
- Informace o konfiguraci, které jsou upraveny pro instalaci jako celek. Informace o konfiguraci jsou spravovány produktem IBM MQ, jako je například soubor `mqs.ini` v systémech Windows, UNIX and Linux nebo část vlastní správy konfigurace, jako např. konfigurační skripty produktu **MQSC** . Zálohování a obnova pomocí archivu souborů.
- Výstup z instalace, jako jsou například trasování, protokoly chyb a soubory FFDC. Soubory se uloží do podadresářů `errors` a `trace` ve výchozím datovém adresáři. Výchozí datový adresář na systémech UNIX and Linux je `/var/mqm`. V systému Windows je výchozím datovým adresářem instalační adresář produktu IBM MQ .

Správce front pro zálohování můžete také použít k provádění pravidelných záloh médií správce front s více instancemi pomocí lineárního protokolování. Záložní správce front neposkytuje obnovu, která je stejně rychlá jako ze zrcadleného systému souborů a neobnoví změny od poslední zálohy. Záložní mechanizmus správce front je vhodnější pro použití ve scénářích zotavení z havárie v režimu offline, než je zotavení správce front po lokalizovaném selhání úložiště.

Kombinování řešení dostupnosti IBM MQ

Aplikace používají jiné funkce produktu IBM MQ ke zlepšení dostupnosti. Správci front s více instancemi doplňují jiné možnosti vysoké dostupnosti.

IBM MQ Klastry zvyšují dostupnost fronty

Můžete zvýšit dostupnost fronty vytvořením více definic fronty klastru; až do jedné z každé fronty v každém správci v klastru.

Předpokládejme, že člen klastru selže, a pak se odešle nová zpráva do fronty klastru. Pokud zpráva *nemá* pro přechod na správce front, který selhal, odešle se zpráva do jiného spuštěného správce front v klastru, který má definici fronty.

Ačkoli klastry výrazně zvyšují dostupnost, existují dva související scénáře selhání, které vedou ke zpoždění zpráv. Sestavení klastru pomocí správců front s více instancemi snižuje možnost opožděného zpoždění zprávy.

Manoované zprávy
Pokud se správce front v klastru nezdaří, žádné další zprávy, které mohou být směrovány do jiných správců front v klastru, jsou směrovány do správce front, který selhal. Zprávy, které již byly odeslány, jsou zakonovány, dokud se správce front, který selhal, znovu spustí.

Afinity

Afinita je termín používaný k popisu informací sdílených mezi dvěma jinak oddělenými výpočty. Existuje například afinita mezi aplikací odesílající zprávu požadavku na server a stejnou aplikací, která očekává zpracování odpovědi. Dalším příkladem může být posloupnost zpráv, zpracování každé zprávy v závislosti na předchozích zprávách.

Pokud odešlete zprávy do sdružených front, je třeba zvážit afinity. Potřebujete odeslat následné zprávy do stejného správce front, nebo může každá zpráva přejít na kteréhokoli člena klastru?

Pokud budete muset odesílat zprávy do stejného správce front v klastru a dojde k selhání, budou zprávy čekat v přenosové frontě odesílatele, dokud se správce front klastru, který selhal, znovu nespustí.

Je-li klastr konfigurován s víceinstanční správci front, bude zpoždění, které čeká na restartování správce front, restartováno, je omezeno na pořadí minut nebo na chvíli, kdy rezervní databáze převezme řízení. Když je rezervní databáze spuštěna, zahájí se zpracování zamalených zpráv, spustí se kanály do nově aktivované instance správce front a zprávy, které čekaly v přenosových frontách, začnou proudit.

Možným způsobem, jak nakonfigurovat klastr k odstranění zpráv zpožděných správcem front se selháním, je nasadit dva různé správce front na každý server v klastru a zajistit, aby jeden z nich byl aktivní a jeden jako záložní instance pro různé správce front. Jedná se o konfiguraci aktivní rezervní databáze a zvyšuje dostupnost klastru.

Kromě výhod snížené administrace a zvýšené rozšiřitelnosti mohou klastry poskytovat další prvky dostupnosti, které doplňují správce front s více instancemi. Klastry jsou chráněny proti jiným typům selhání, které ovlivňují jak aktivní, tak i rezervní instance správce front.

Nepřerušená služba
Klastr poskytuje nepřerušenou službu. Nové zprávy přijaté klastrem se odešlou do aktivních správců front, které mají být zpracovány. Nespoléhejte se na správce front s více instancemi, aby poskytoval nepřerušovanou službu, protože vyžaduje, aby správce front v pohotovostním režimu zjistil selhání a dokončil své spuštění, aby bylo možné kanály znovu připojit, a aby byly znovu odeslány selhané dávky zpráv.

Lokalizovaný výpadek
Existují praktická omezení pro to, jak daleko od sebe mohou být aktivní, záložní a servery systémů souborů, protože je třeba interaktivně pracovat s rychlostí milisekund, aby bylo možné dosáhnout přijatelného výkonu.

Klastrované správce front vyžadují zrychlení interakce v řádu mnoha sekund a mohou být geograficky rozptýleny kdekoli na světě.

Operační chyba
Použitím dvou různých mechanizmů pro zvýšení dostupnosti snížíte pravděpodobnost, že provozní chyba, jako např. lidská chyba, bude ohrožovat vaše úsilí o dosažení dostupnosti.

Skupiny sdílení front zvyšují dostupnost zpracování zpráv

z/OS Skupiny sdílení front, které jsou k dispozici pouze v produktu z/OS, umožňují skupině správců front sdílet obsluhování fronty. Dojde-li k selhání jednoho správce front, budou ostatní správci front nadále zpracovávat všechny zprávy ve frontě. Správci front s více instancemi nejsou v produktu z/OS podporovány a doplňují skupiny sdílení front pouze jako součást širší architektury systému zpráv.

IBM MQ Klienti zvyšují dostupnost aplikací

Programy produktu IBM MQ MQI client se mohou připojovat k různým správcům front ve skupině správců front na základě dostupnosti správce front, vah připojení a afinit. Spuštěním aplikace na jiném počítači než ten, na kterém běží správce front, můžete zlepšit celkovou dostupnost řešení tak dlouho, dokud existuje způsob opětovného připojení aplikace, pokud je instance správce front připojená k selhání.

Skupiny správců front se používají ke zvýšení dostupnosti klienta odpojením klienta od správce front, který je zastaven, a vyrovnávání zátěže klienta v rámci skupiny správců front, spíše jako sprejer IP. Klientská aplikace nesmí mít žádné afinity s nezdařeným správcem front, jako je například závislost na konkrétní frontě, nebo nemůže pokračovat ve zpracování.

Automatické opětovné připojení klientů a správce front s více instancemi zvyšují dostupnost klientů tím, že řeší některé problémy s afinitou. Prostředí IBM MQ classes for Java nepodporuje automatické opětovné připojování klientů.

Můžete nastavit volbu `MQCNO` `MQCNO_RECONNECT_Q_MGR`, chcete-li přinutit klienta, aby se znovu připojil ke stejnému správci front:

1. Pokud dříve připojený správce front instance není spuštěn, pokus o připojení se znovu pokusí, dokud nebude správce front spuštěn znovu.
2. Je-li správce front konfigurován jako správce front s více instancemi, pak se klient znovu připojí k aktivní instanci.

Po automatickém opětovného připojení ke stejnému správci front byla obnovena velká část informací o stavu, které správce front v zastoupení klienta držel, například fronty, které byly otevřeny, a téma, k jehož odběru bylo přihlášeno, obnoveno. Pokud klient otevřel dynamickou odpověď-do fronty pro přijetí odpovědi na požadavek, je obnoveno připojení k frontě pro odpověď.

V 9.1.0 MQ Adv. Linux Vysoká dostupnost RDQM

RDQM (replikovaný správce datových front) je řešení vysoké dostupnosti, které je k dispozici na platformách Linux .

Konfigurace RDQM se skládá ze tří serverů konfigurovaných ve skupině s vysokou dostupností (HA), přičemž každá z nich je instancí správce front. Jedna instance je spuštěný správce front, který synchronně replikuje svá data do ostatních dvou instancí. Pokud server, na kterém je spuštěn tento správce front, selže, spustí se jiná instance správce front a má aktuální data, se kterými bude pracovat. Tyto tři instance správce front sdílejí plovoucí adresu IP, takže klienti je třeba konfigurovat pouze s jednou adresou IP. V jednom okamžiku může být spuštěna pouze jedna instance správce front, a to i v případě, že se skupina s vysokou dostupností stane dělenou vzhledem k problémům se sítí. Server, na kterém běží správce front, je znám jako 'primary', každý z ostatních dvou serverů je známý jako 'sekundární'.

Tři uzly se používají k výraznému snížení možnosti rozdělení do mozku situace. V případě mezi dvěma uzly může dojít k přerušení rozdělení systému s vysokou dostupností do dvou uzlů, je-li přerušena konektivita mezi dvěma uzly. S žádnou konektivitou nemohou oba uzly ve stejnou chvíli spustit správce front a hromadit různá data. Když je obnoveno připojení, existují dvě různé verze dat ('split-mozek') a ruční zásah je nutný k rozhodnutí, kterou datovou sadu uchovat, a které se mají vyřadit.

RDQM používá systém tří uzlů s kvótou, aby se zabránilo situaci split-mozku. Uzly, které mohou komunikovat alespoň s jedním z ostatních uzlů, tvoří kvorum. Správci front lze spustit pouze na uzlu, který má kvorum. Správce front nemůže být spuštěn na uzlu, který není připojen k alespoň jednomu uzlu, takže nelze nikdy spustit ve dvou uzlech současně:

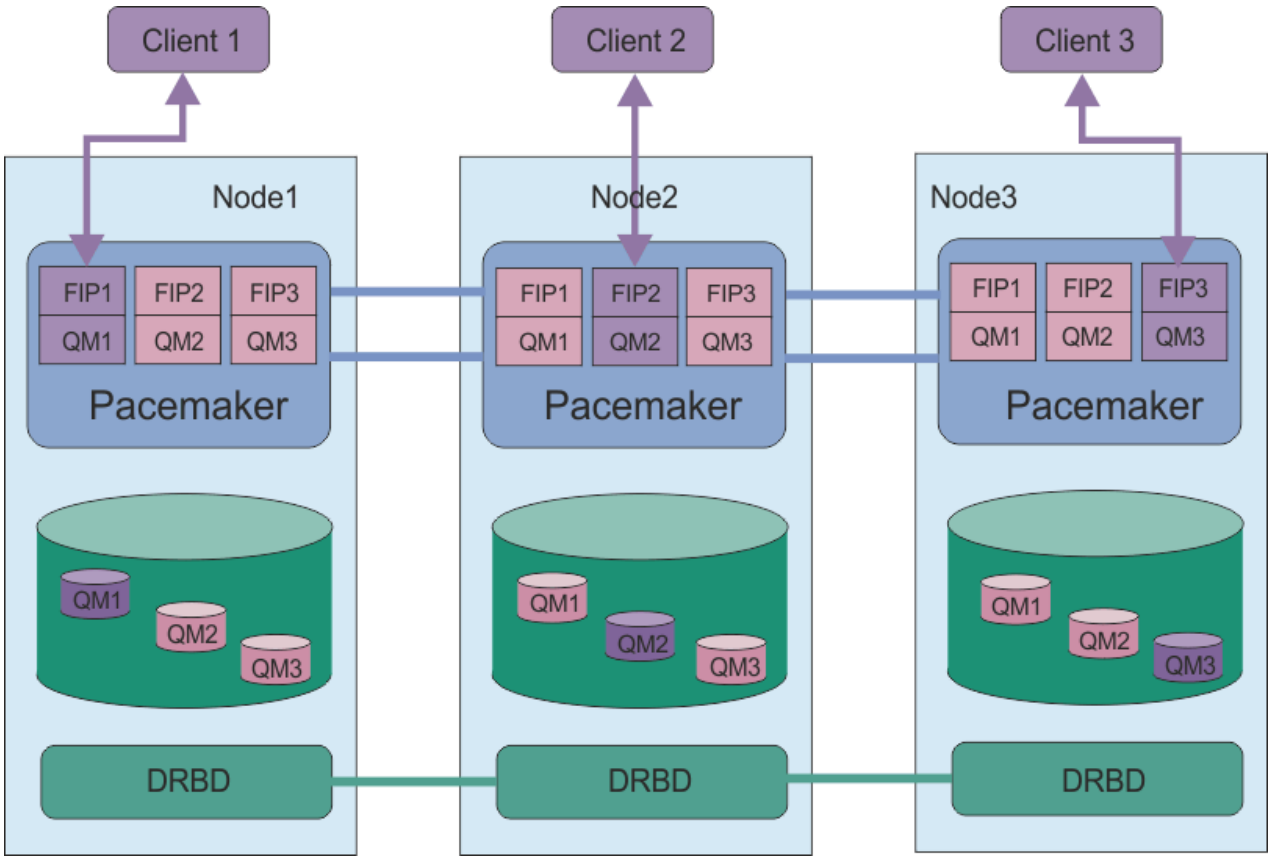
- Dojde-li k selhání jednoho uzlu, může být správce front spuštěn na jednom z dalších dvou uzlů. Pokud selžou dva uzly, nemůže být správce front spuštěn na zbývajícím uzlu, protože uzel nemá kvorum (zbývající uzel nemůže určit, zda došlo k selhání ostatních dvou uzlů, nebo jsou stále spuštěné a má ztracenou konektivitu).
- Pokud jeden uzel ztratí propojitelnost, nemůže být správce front spuštěn na tomto uzlu, protože uzel nemá kvorum. Správce front může být spuštěn na jednom ze zbývajících dvou uzlů, které mají kvorum. Pokud všechny uzly ztratí propojitelnost, správce front se nebude moci spustit na žádném z uzlů, protože žádný z uzlů není kvorum.

Poznámka: Produkt IBM MQ Console nepodporuje replikované správce datových front. Můžete použít produkt IBM MQ Explorer s replikovanými správci datových front, ale to nezobrazuje informace specifické pro funkce RDQM.

Skupině konfigurace tří uzlů je obsloužen Pacemaker. Replikace mezi třemi uzly se zpracovává pomocí DRBD. (Informace o parametru DRBD naleznete v příručce https://clusterlabs.org/pacemaker/) o Pacemaker a https://docs.linbit.com/docs/users-guide-9.0/ .)

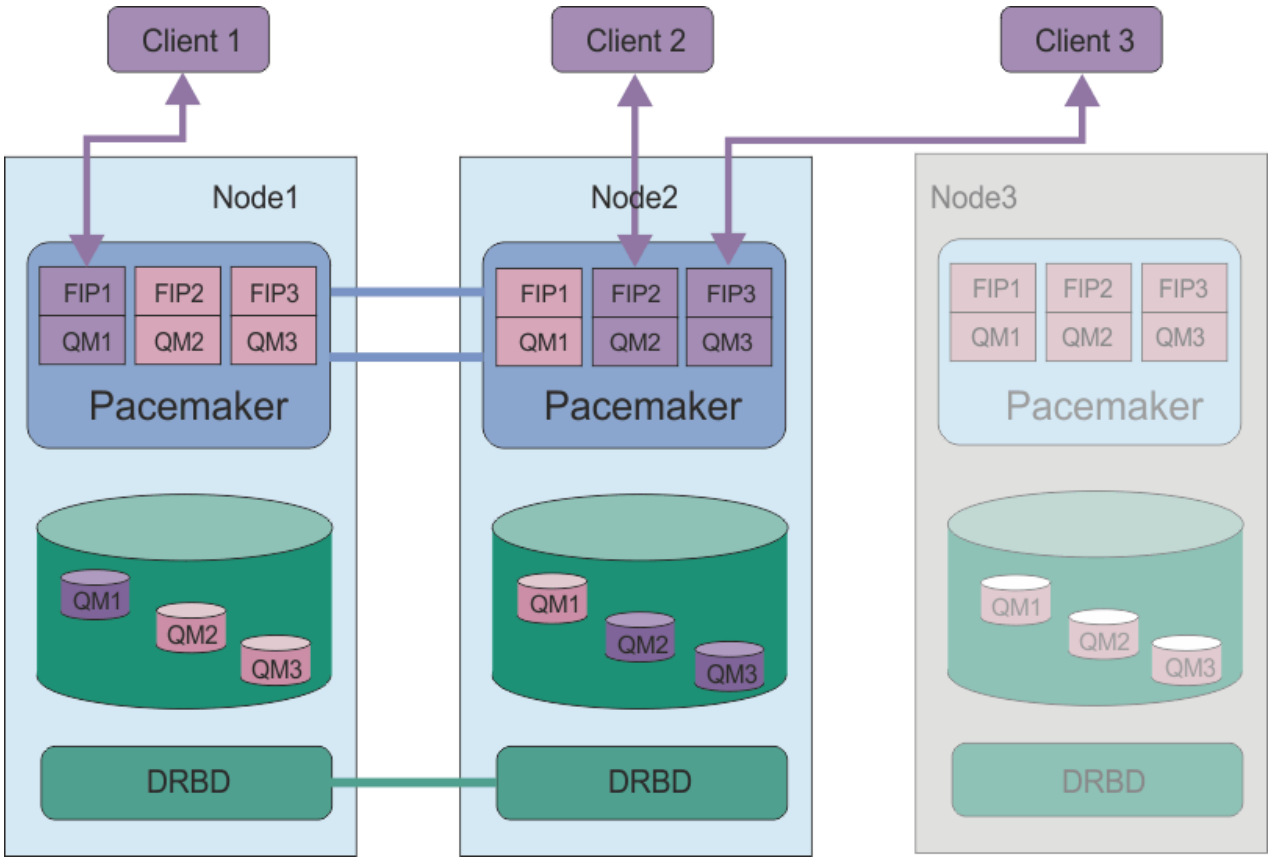
Správce replikovaných datových front můžete zálohovat s použitím procesu popsaného v tématu “Zálohování dat správce front” na stránce 602. Zastavení správce front a zálohování nemá žádný vliv na monitorování uzlu prováděné konfigurací RDQM.

Následující obrázek ukazuje typickou implementaci s RDQM spuštěným na každém ze tří uzlů ve skupině HA.



Obrázek 81. Příklad skupiny HA se třemi moduly RDQM

Na dalším obrázku došlo k selhání uzlu Node3 , odkazy Pacemaker byly ztraceny a správce front QM3 je spuštěn na uzlu Node2 .



Obrázek 82. Příklad po selhání uzlu node3

Poznámka: Když správci front selžou v jiném uzlu, zachovávají stav, který měli při překonání selhání. Spuštěné správce front jsou spuštění správci front, kteří byli zastaveni, i nadále zastaveni.

Související úlohy

Instalace RDQM (replikovaných správců datových front)

Upgrade RDQM (replikovaných správců datových front)

Migrace správců replikovaných datových front

V 9.1.0 Linux

Požadavky pro řešení RDQM HA

Před konfigurací skupiny s vysokou dostupností RDQM je třeba splnit řadu požadavků.

Systémové požadavky

Před konfigurací skupiny HA RDQM musíte dokončit některé konfigurace na každém ze tří serverů, které jsou součástí skupiny HA.

- Každý uzel vyžaduje skupinu disků s názvem `drbdpool`. Úložiště pro každého správce replikovaných datových front je přiděleno jako samostatný logický svazek na správce front z této skupiny disků. Pro nejlepší výkon by tato skupina disků měla být tvořena jedním nebo více fyzickými disky, které odpovídají interním diskovým jednotkám (pokud možno SSD). Můžete vytvořit `drbdpool` před nebo po instalaci řešení vysoké dostupnosti RDQM, ale musíte vytvořit `drbdpool` před tím, než budete ve skutečnosti vytvořit RQMs. 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
```

Konkrétně zkontrolujte, že v šestém sloupci atributů není žádný znak c (tedy `wz--nc`). Hodnota c udává, že je povoleno klastrování, a pokud ano, musíte skupinu disků odstranit a znovu ji vytvořit bez klastrování.

- Poté, co jste vytvořili skupinu disků `drbdpool` , nedělejte s ní nic jiného. Produkt IBM MQ spravuje logické svazky vytvořené v produktu `drbdpool`a jak a kde jsou připojeny.
- 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 k 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 zátěži všech replikovaných správců datových front spuštěných ve skupině HA.

  Skupinu s vysokou dostupností můžete nakonfigurovat tak, aby stejná adresa IP byla použita pro všechna tři rozhraní, pro každé rozhraní se použije samostatná adresa IP nebo se použije stejná adresa IP pro primární a alternativní adresu IP a pro rozhraní replikace.

  Pro maximální odolnost proti poruchám by tato rozhraní měla být nezávislá na kartách síťového rozhraní (NIC).
- DRBD vyžaduje, aby každý uzel ve skupině HA měl platný internetový název hostitele (hodnota vrácená produktem `uname -n`), jak je definováno v RFC 952, novelizovaný RFC 1123.
- Je-li mezi uzly ve skupině HA brána firewall, musí brána firewall umožňovat provoz mezi uzly na řadě portů. K dispozici je ukázkový skript `/opt/mqm/samp/rdqm/firewalld/configure.sh`, který otevře potřebné porty, pokud provozujete standardní bránu firewall v systému RHEL. Skript musíte spustit jako `root`. Pokud používáte nějakou jinou bránu firewall, prozkoumejte definice služeb `/usr/lib/firewalld/services/rdqm*` , abyste viděli, které porty je třeba otevřít.
- Pokud systém používá SELinux v režimu Enforcing, musíte spustit tento příkaz:

```
semanage permissive -a drbd_t
```

Síťové požadavky

Doporučuje se umístit tři uzly ve skupině HA RDQM ve stejném datovém středisku.

Pokud se rozhodnete vyhledat uzly v různých datových centrech, uvědomte si následující omezení:

- Výkon se rychle zhoršuje se zvyšující se latencí mezi datovými centry. Přestože společnost IBM bude podporovat latenci až 5 ms, může dojít k zjištění, že výkon aplikace nemůže tolerovat více než 1 až 2 ms latence.
- Data odeslaná přes replikační odkaz se nevztahují na žádné další šifrování, které by mohlo být na místě, které by mohlo být použito při použití serveru IBM MQ AMS.

Můžete nakonfigurovat plovoucí adresu IP, abyste umožnili klientovi použít stejnou adresu IP pro replikovaný správce datových front (RDQM) bez ohledu na to, který uzel ve skupině HA běží na. Plovoucí adresa se váže k pojmenovanému fyzickému rozhraní na primárním uzlu pro RDQM. Pokud dojde k selhání RDRQM a primární uzel se stane primárním uzlem, bude plovoucí adresa IP svázána s rozhraním stejného názvu na novém primárním uzlu. Fyzická rozhraní na třech uzlech musí mít všechny stejné názvy a náležejí do stejné podsítě jako plovoucí adresa IP.

Požadavky na uživatele pro konfiguraci klastru

Skupinu RDQM HA můžete nakonfigurovat jako uživatele `root`. Pokud se nechcete konfigurovat jako `root`, budete namísto toho konfigurovat jako uživatele ve skupině `mqm` . Aby mohl uživatel produktu `mqm` konfigurovat klastr RDQM, musíte splnit tyto požadavky:

- Uživatel `mqm` musí být schopen použít příkaz sudo ke spuštění příkazů na každém ze tří serverů, které tvoří skupinu HA RDQM.

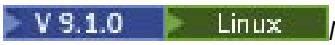
- Pokud může uživatel produktu mqm použít SSH bez hesla ke spouštění příkazů na každém ze tří serverů, které tvoří skupinu RDQM HA, pak uživatel musí spouštět příkazy pouze na jednom ze serverů.
- Pokud pro uživatele produktu mqm nakonfigurujete heslo SSH bez hesla, musí mít tento uživatel stejné UID na všech třech serverech.

Příkaz sudo je třeba nakonfigurovat tak, aby uživatel produktu mqm mohl spouštět následující příkazy s oprávněním root:

```
/opt/mqm/bin/crtmqm
/opt/mqm/bin/dltmqm
/opt/mqm/bin/rdqmadm
/opt/mqm/bin/rdqmstatus
```

Požadavky na uživatele pro práci se správci front

Chcete-li vytvořit, odstranit nebo konfigurovat replikované správce datových front (RQMs), musíte použít ID uživatele, které patří do skupin produktů mqm a haclient (skupina haclient se vytvoří během instalace Pacemaker).



Nastavení zabezpečení SSH bez hesla

Můžete nastavit zabezpečení SSH bez hesla, abyste měli v jednom uzlu ve skupině s vysokou dostupností pouze příkazy pro konfiguraci problému.

Informace o této úloze

Chcete-li nastavit zabezpečení SSH bez hesla, musíte nakonfigurovat ID produktu mqm na každém uzlu a poté generovat klíč na každém uzlu pro tohoto uživatele. Poté rozdělte klíče do jiných uzlů a otestujte připojení tak, že přidáte každý uzel do seznamu známých hostitelů. Nakonec uzamknete ID mqm .

Poznámka: Pokyny předpokládají, že definujete skupinu HA se samostatným primárním, alternativním a replikačním rozhraním, a proto definujete přístup SSH bez hesla přes primární a alternativní rozhraní. Pokud plánujete konfigurovat systém s jednou adresou IP, pak nadefinujete přístup SSH bez hesla přes toto jediné rozhraní.

Postup

1. Na každém ze tří uzlů nastavte uživatele mqm pomocí následujícího postupu a vygenerujte 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 produktu mqm :

   ```
   passwd mqm
   ```

   d) Spusťte interaktivní shell jako mqm:

   ```
   su mqm
   ```

   e) Vygenerujte ověřovací klíč produktu mqm :

   ```
   ssh-keygen -t rsa -f /home/mqm/.ssh/id_rsa -N ''
   ```

2. U každého ze tří uzlů následujícím postupem přidejte klíč uzlu do ostatních dvou uzlů a otestujte připojení pro jednotlivé uzly primární a (je-li použita) alternativní adresy:
   a) Přidejte klíč do vzdálených uzlů

```
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 uzly 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 se zobrazí výzva k potvrzení, že chcete pokračovat. Potvrďte, že každý z nich aktualizuje known_hosts. Musíte to dokončit, dříve než se pokusíte nakonfigurovat skupinu HA pomocí SSH bez hesla.

c) Ukončete interaktivní shell jako mqm:

```
exit
```

3. Na každém uzlu jako uživatel root odeberte heslo produktu mqm pomocí následujícího postupu a zamkněte ID:

a) Odeberte heslo produktu mqm :

```
passwd -d mqm
```

b) Zamknout mqm:

```
passwd -l mqm
```

4. V každém uzlu jako uživatel root proveďte následující kroky, abyste nastavili přístup pro příkaz sudo pro uživatele produktu mqm :

a) Upravte soubor sudoers pomocí příkazu **visudo** :

```
visudo
```

b) Vyhledejte řádek "*## Allows people in group wheel to run all commands*" a přidejte následující text pod tento řádek:

```
#%mqm    ALL=(ALL)       ALL
```

c) Vyhledejte řádek "*## Same thing without a password*" a přidejte následující text pod tento řádek:

```
%mqm            ALL=(ALL)       NOPASSWD: ALL
```

V 9.1.0 Linux

Definování klastru Pacemaker (HA group)

Skupina s vysokou dostupností je klastr Pacemaker . Klastr Pacemaker definujete úpravou souboru /var/mqm/rdqm.ini a spuštěním příkazu **rdqmadm** .

Informace o této úloze

Informace o Pacemakerviz https://clusterlabs.org/pacemaker/ . Můžete vytvořit klastr Pacemaker jako uživatel ve skupině mqm , pokud může uživatel produktu mqm použít produkt sudo. Pokud se uživatel může také SSH na každém serveru bez hesla, pak stačí upravit soubor rdqm.ini a spustit příkaz **rdqmadm** na jednom ze serverů a vytvořit klastr Pacemaker . Jinak musíte vytvořit soubor a spustit tento příkaz jako root na každém ze serverů, které mají být uzly.

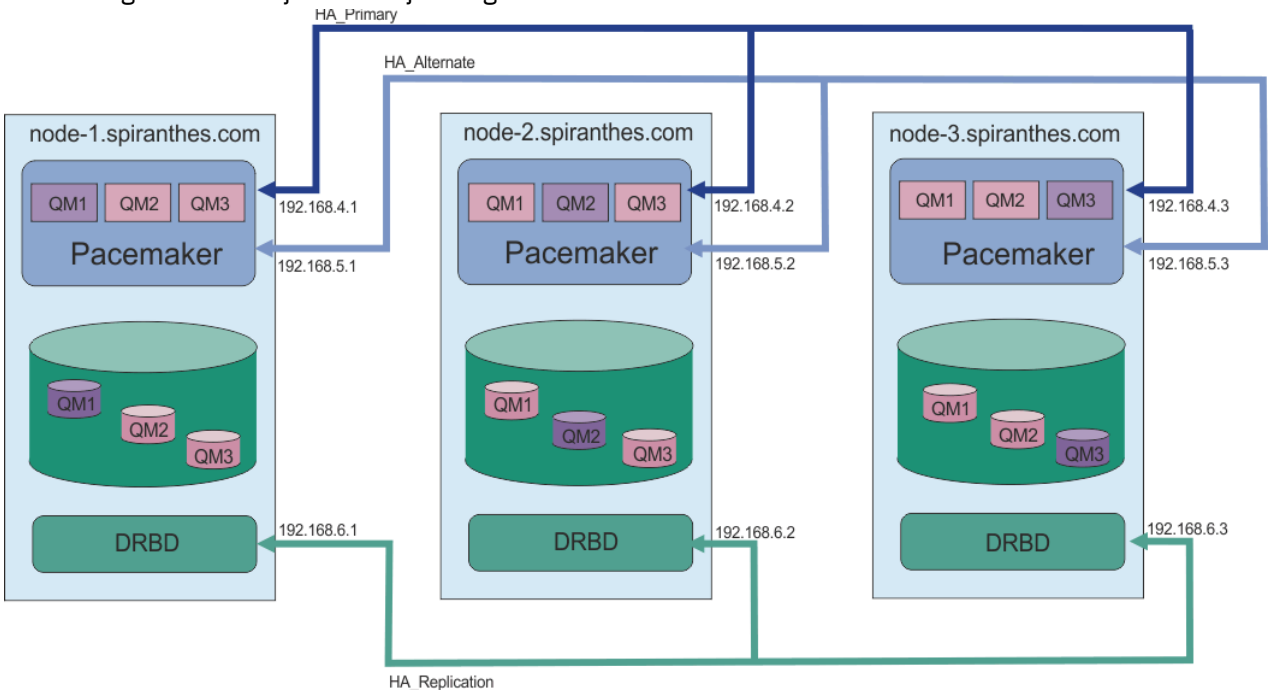
Soubor rdqm.ini poskytuje adresy IP pro všechny uzly v klastru Pacemaker . Můžete definovat rozhraní HA_Primary a HA_Secondary , která se používají pro Pacemaker k monitorování systému, ale Pacemaker může místo toho použít toto rozhraní replikace s názvem HA_Replicationpro tento

účel, je-li to nutné. Rozhraní produktu `HA_Replication` musí mít dostatečnou šířku pásma pro podporu požadavků replikace vzhledem k očekávané zátěži všech modulů RDQM spuštěných ve skupině HA.

Následující ukázkový soubor zobrazuje konfiguraci pro příklad klastru Pacemaker , který používá samostatnou adresu IP pro každé rozhraní:

```
Node:
  HA_Primary=192.168.4.1
  HA_Alternate=192.168.5.1
  HA_Replication=192.168.6.1
Node:
  HA_Primary=192.168.4.2
  HA_Alternate=192.168.5.2
  HA_Replication=192.168.6.2
Node:
  HA_Primary=192.168.4.3
  HA_Alternate=192.168.5.3
  HA_Replication=192.168.6.3
```

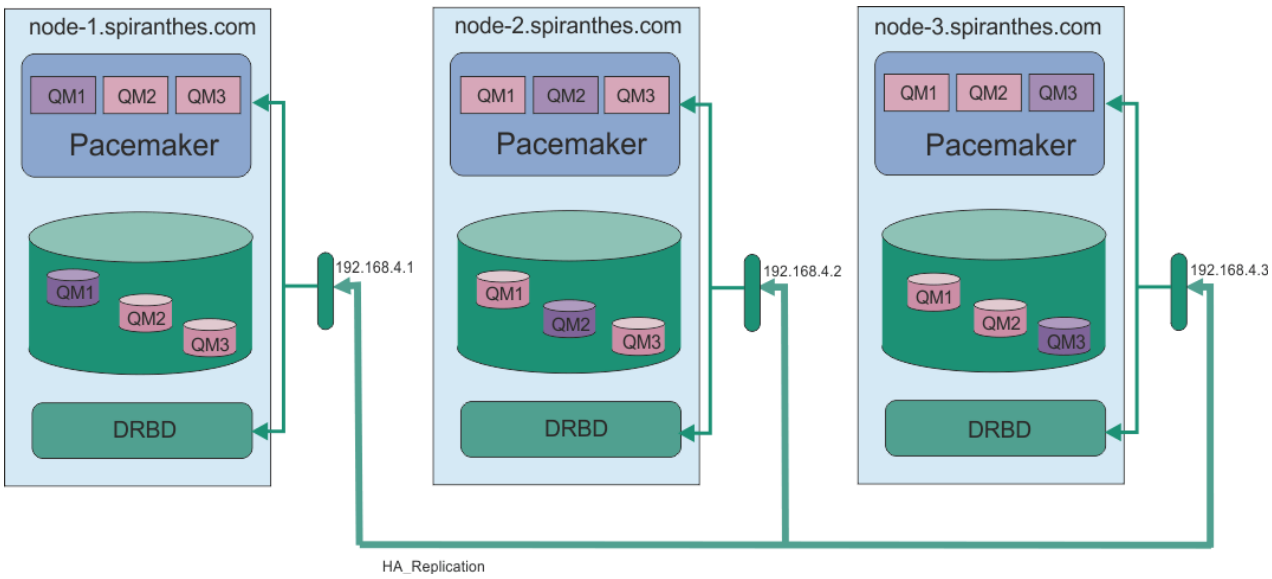
Tato konfigurace ilustruje následující diagram:



Následující ukázkový soubor zobrazuje konfiguraci pro příklad klastru Pacemaker , který používá rozhraní produktu `HA_Replication` pro monitorování. V tomto případě uvedete pouze rozhraní produktu `HA_Replication` :

```
Node:
  HA_Replication=192.168.4.1
Node:
  HA_Replication=192.168.4.2
Node:
  HA_Replication=192.168.4.3
```

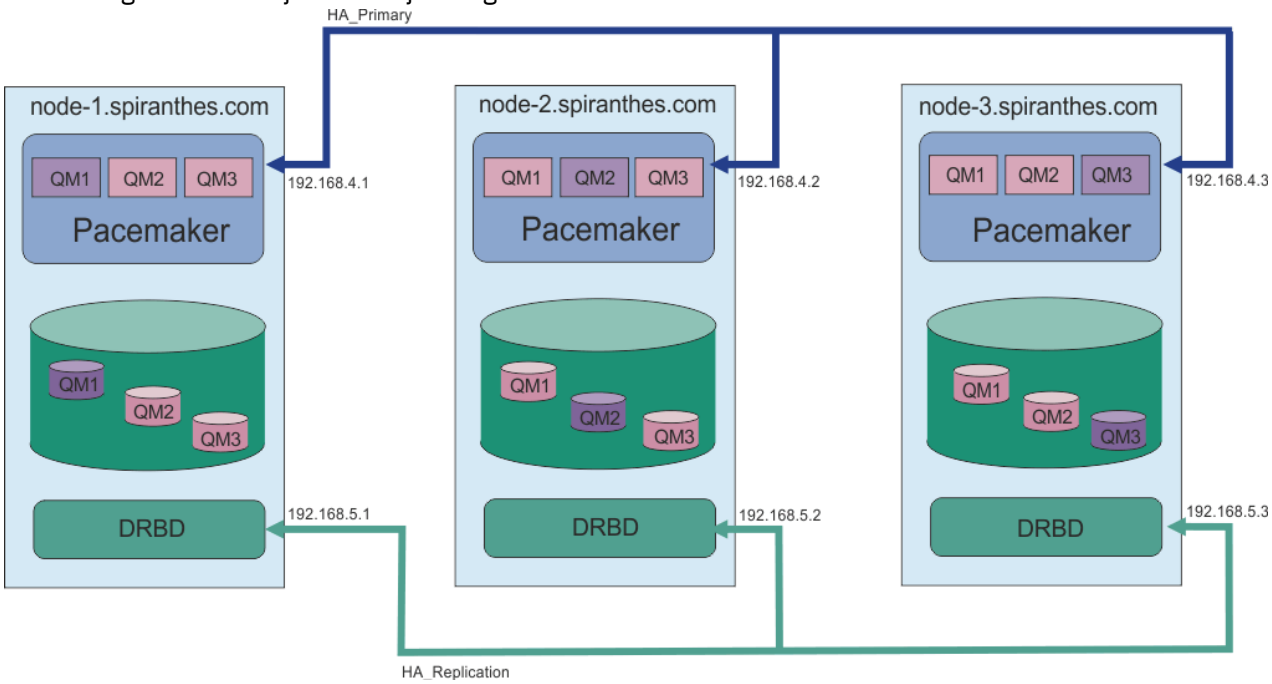
Tato konfigurace ilustruje následující diagram:



Pokud jste chtěli použít dvě adresy IP, váš soubor `rdqm.ini` má pro každý uzel pole `HA_Primary` a `HA_Replication` , ale žádné pole `DO_Alternate` :

```
Node:
  HA_Primary=192.168.4.1
  HA_Replication=192.168.5.1
Node:
  HA_Primary=192.168.4.2
  HA_Replication=192.168.5.2
Node:
  HA_Primary=192.168.4.3
  HA_Replication=192.168.5.3
```

Tato konfigurace ilustruje následující diagram:



Pořadí, ve kterém určujete uzly, musí být ve všech souborech `rdqm.ini` ve vaší konfiguraci shodné. Vaše tři uzly musí mít společný pohled na to, který z nich je Node1, který je Node2 atd.

Procedura

- Chcete-li definovat klastr Pacemaker jako uživatel `root`:
  a) Upravte soubor `/var/mqm/rdqm.ini` na jednom ze tří serverů tak, aby tento soubor definoval klastr.
  b) Zkopírujte tento 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 uživatel ve skupině `mqm` na každém uzlu, postupujte takto:
  a) Ujistěte se, že uživatel `mqm` může použít příkaz **sudo** ke spouštění příkazů.
  b) Upravte soubor `/var/mqm/rdqm.ini` na jednom ze tří serverů tak, aby soubor definovala klastr Pacemaker .
  c) Zkopírujte `/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 příkaz **sudo** ke spouštění příkazů a může se volitelně připojit ke každému serveru pomocí SSH bez hesla.
  b) Upravte soubor `/var/mqm/rdqm.ini` na jednom ze tří serverů tak, aby soubor definovala klastr Pacemaker .
  c) Spusťte tento příkaz:

```
rdqmadm -c
```

Související odkazy
rdqmadm (spravovat replikovaný klastr správce datových front)

V 9.1.0 Linux *Odstranění klastru Pacemaker (skupina HA)*
Skupina s vysokou dostupností je klastr Pacemaker . Konfiguraci klastru Pacemaker lze odstranit spuštěním příkazu **rdqmadm** s volbou `-u` .

Informace o této úloze

Konfiguraci klastru Pacemaker nelze odstranit, pokud na některém z uzlů stále existují replikované správce datových front.

Procedura

- Chcete-li odstranit konfiguraci klastru Pacemaker , zadejte z libovolného uzlu následující příkaz:

```
rdqmadm -u
```

Související odkazy
rdqmadm (spravovat replikovaný klastr správce datových front)

V 9.1.0 Linux ***Vytvoření agenta HA RDQM***
Pomocí příkazu **crtmqm** vytvoříte replikovaný správce datových front o vysoké dostupnosti (RDQM).

Informace o této úloze

Pokud uživatel mqm může použít příkaz sudo, můžete vytvořit replikovaný správce datových front (RDQM) s vysokou dostupností jako uživatel ve skupině `mqm` . Pokud může uživatel také SSH do každého uzlu bez

hesla, pak stačí spustit příkaz pro vytvoření RDRQM na jednom uzlu k vytvoření RDQM na všech třech uzlech. Jinak musíte být `root` , abyste vytvořili RDQM, a musíte spustit příkazy na všech třech uzlech.

Procedura

- Chcete-li vytvořit RDQM jako uživatele ve skupině `mqm` , postupujte takto:
  a) Ujistěte se, že uživatel produktu `mqm` může použít příkaz **sudo** ke spouštění 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 replikovaného správce datových front. Volitelně můžete určit velikost systému souborů správce front (to znamená velikost logického disku, který je vytvořen ve skupině svazků drbdpool).

  Příkaz se pokusí použít SSH, aby se připojil k ostatním uzlům v klastru jako uživatel `mqm` . Je-li připojení úspěšné, vytvoří se v uzlech sekundární instance správce front. Jinak musíte vytvořit sekundární instance a poté spustit příkaz **`crtmqm -sx`** (jak je popsáno pro uživatele `root`).
- Chcete-li vytvořit RDQM jako uživatele `root`:
  a) Zadejte následující příkaz na každém z uzlů, které jsou hostiteli sekundárních instancí RDQM:

  ```
  crtmqm -sxs [-fs FilesystemSize] qmname
  ```

  kde *qmname* je název replikovaného správce datových front. Volitelně můžete určit velikost systému souborů správce front (to znamená velikost logického disku, který je vytvořen ve skupině svazků drbdpool). Musíte zadat stejnou velikost systému souborů pro RDQM na všech třech uzlech ve skupině HA.

  Příkaz vytvoří sekundární instanci RDQM.
  b) Na zbývajícím uzlu zadejte tento příkaz:

  ```
  crtmqm -sx [-fs FilesystemSize] qmname
  ```

  kde *qmname* je název replikovaného správce datových front. Volitelně můžete určit velikost systému souborů pro správce front.

  Příkaz určí, zda sekundární instance správce front existuje na ostatních dvou uzlech. Pokud existují sekundární logické jednotky, příkaz vytvoří a spustí primárního správce front. Pokud sekundární servery neexistují, dostanete pokyn 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 replikovaného správce datových front.

  Poznámka: Když vytvoříte RDQM, je pro odkaz na replikaci přiděleno další volné číslo portu nad 7000. Je-li zjištěno, že zvolený port je použit jinou aplikací, příkaz **`crtmqm`** selže s chybou AMQ6543 a tento port je přidán do vylučovacího seznamu. Musíte odstranit sekundární instance správce front a pak znovu spustit příkaz **`crtmqm`** .

Související odkazy

crtmqm

V 9.1.0 Linux *Odstranění RDQM HA*

K odstranění replikovaného správce datových front (RDQM) s vysokou dostupností použijte příkaz **`dltmqm`** .

Informace o této úloze

Příkaz musíte spustit, chcete-li vymazat RDQM na primárním uzlu RDQM. RDQM musí být ukončen první. Příkaz můžete spustit jako uživatel mqm, pokud má tento uživatel potřebná oprávnění k příkazu

sudo. Jinak musíte spustit příkaz jako uživatel root. Po odstranění prostředků přidružených k primárnímu správci front se příkaz pokusí odstranit sekundární správce front pomocí služby SSH, aby se mohl připojit k ostatním uzlům. Pokud se toto odstranění nezdaří, je třeba proces dokončit ručně spuštěním příkazu `dltmqm` na ostatních uzlech. Na sekundárním uzlu se příkaz nezdaří, pokud primární správce front dosud nebyl odstraněn.

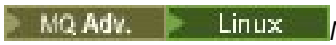
Procedura

- Chcete-li odstranit RDQM, zadejte tento příkaz:

```
dltmqm RDQM_name
```

Související odkazy

dltmqm



Migrace správce front s cílem stát se správcem front HA RQM

Existující správce front můžete migrovat tak, aby se stal replikovaným správcem front vysoké dostupnosti (RDS) tím, že zálohuje trvalá data a poté obnoví data do nově vytvořeného správce front RDQM, který má stejný název.

Informace o této úloze

Replikované správci datových front HA vyžadují vyhrazený logický svazek (systém souborů) a konfiguraci replikace disků a řízení HA. Tyto komponenty jsou konfigurovány pouze v případě, že je vytvořen nový správce front. Existující správce front lze migrovat tak, aby používal RDQM tak, že zálohuje trvalá data a poté obnoví data do nově vytvořeného správce front RDQM, který má stejný název. Tento postup zachovává konfiguraci správce front, stav a trvalé zprávy v době vytvoření zálohy.

Poznámka: Migraci správce front můžete provést pouze z verze produktu IBM MQ , která je stejná nebo nižší než verze, na které je nainstalován produkt RDQM. Operační systém a architektura musí být také stejné. Jinak je třeba na cílové platformě vytvořit nového správce front, viz téma Přesun správce front do jiného operačního systému.

Před migrací správce front byste měli splnit následující podmínky:

- Vyhodnoťte své požadavky vysoké dostupnosti a prohlédněte si téma “Vysoká dostupnost RDQM” na stránce 513.
- Zkontrolujte aplikace a správce front, kteří se připojují ke správci front. Zvažte změny nezbytné pro směrování připojení k uzlu RDQM, kde je spuštěn správce front. Například, pokud nakonfigurujete vysokou dostupnost RDQM, můžete zvážit použití plovoucí adresy IP, viz “Vytvoření a odstranění plovoucí adresy IP” na stránce 529.
- Zajistěte nebo identifikujte existující uzly RDQM pro zvolenou konfiguraci. Informace o systémových požadavcích pro RDQM viz “Požadavky pro řešení RDQM HA” na stránce 515.
- Nainstalujte produkt IBM MQ Advanced, který obsahuje funkci RDQM, na každém uzlu.
- Konfigurujte konfiguraci skupiny RDQM s vysokou dostupností, viz “Definování klastru Pacemaker (HA group)” na stránce 518.
- Volitelně ověřte konfiguraci RDQM pomocí správce testovací fronty, který lze poté odstranit. Testování konfigurace se doporučuje identifikovat a vyřešit případné problémy před migrací správce front.
- Zkontrolujte konfiguraci zabezpečení správce front a poté replikujte požadované lokální uživatele a skupiny do každého uzlu RDQM.
- Zkontrolujte správce front a konfiguraci kanálu a zjistěte, zda se používají uživatelské procedury rozhraní API, ukončení kanálu nebo ukončení převodu dat. Nainstalujte požadované uživatelské procedury na každý uzel RDQM.
- Zkontrolujte všechny definované služby správce front, pak nainstalujte a nakonfigurujte požadované procesy na každém uzlu RDQM.

Postup

1. Vytvořte zálohu stávajícího správce front:
   a) Zastavte existujícího správce front zadáním příkazu wait shutdown `endmqm -w`nebo příkazem okamžitého ukončení práce systému `endmqm -i`. Tento krok je důležitý pro zajištění konzistence dat v záloze.
   b) Určete umístění datového adresáře správce front pomocí zobrazení konfiguračního souboru IBM MQ , `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`naleznete v tématu “IBM MQ konfigurační soubor mqs.ini” na stránce 82.

      Vyhledejte sekci `QueueManager` pro správce front v souboru. Pokud stanza obsahuje klíč s názvem `DataPath` , pak jeho hodnota je datový adresář správce front. Pokud klíč neexistuje, může být datový adresář správce front určen pomocí hodnot klíčů `Prefix` a `Directory` . Datový adresář správce front je zřetězením těchto hodnot ve tvaru *předpona*/qmgrs/*adresář*. Další informace o sekci QueueManager viz “QueueManager sekce souboru mqs.ini” na stránce 93.
   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, který je jediným obdobím (tečka):

      ```
      tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
      ```

   d) Určete umístění adresáře protokolu správce front pomocí zobrazení konfiguračního souboru správce front IBM MQ `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front qm.ini” na stránce 95.

      Adresář protokolu správce front je definován jako hodnota klíče `LogPath` ve stanze `Log` . Informace o stanze viz “Sekce protokolu souboru qm.ini” na stránce 122.
   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, který je jediným obdobím (tečka):

      ```
      tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
      ```

   f) Vytvořte zálohu všech úložišť certifikátů používaných správcem front, nejsou-li umístěny v datovém adresáři správce front. Ujistěte se, že je zálohovaný jak soubor databáze klíčů, tak soubor pro uložení hesla. Informace o úložišti klíčů správce front najdete v tématu Úložiště klíčů SSL/TLS a Nalezení úložiště klíčů pro správce front. Informace o umístění úložiště klíčů AMS, je-li správce front konfigurován pro použití zachycování agenta MCA (AMS Message Channel Agent), najdete v tématu WebSphere Message Channel Agent (MCA) interception.
   g) Existující správce front již není požadován, takže jej lze odstranit. Je-li to možné, měli byste odstranit pouze existujícího správce front poté, co byl úspěšně obnoven na cílovém systému. Odložení odstranění zajišťuje, že správce front může být restartován, pokud se proces migrace nedokončí úspěšně.

      Poznámka: Pokud odložíte odstranění existujícího správce front, nerestartujte jej. Je důležité, aby správce front byl ukončen, protože během migrace byly ztraceny další změny jeho konfigurace nebo stavu.
2. Připravte primární uzel RDQM:
   a) Vytvořte nového správce front RDQM se stejným názvem, jako má správce front, kterého jste zálohovali. Ujistěte se, že systém souborů alokovaný pro správce front RDQM produktem **`crtmqm`** je dostatečně velký, aby obsahoval data, primární protokoly a sekundární protokoly pro existujícího správce front a navíc některé další prostory pro budoucí rozšíření. Informace o tom, jak vytvořit správce front RDQM, viz “Vytvoření agenta HA RDQM” na stránce 521.
   b) Určete primární uzel RDRQM pro správce front. Informace o tom, jak určit primární uzel, najdete v tématu rdqmstatus (display RDRQM status).
   c) Je-li správce front RDQM spuštěn v primárním uzlu RDQM, zastavte jej pomocí příkazu `endmqm -w` nebo `endmqm -i` .

d) Na primárním uzlu RDQM určete umístění dat a adresářů protokolu pro správce front RDQM (použijte metody popsané v krocích 1b a 1d).

e) Na primárním uzlu RDQM odstraňte obsah adresářů správce front RDQM a adresářů protokolu, ale ne samotných adresářů.

3. Obnovte správce front v primárním uzlu RDQM:

a) Zkopírujte zálohy dat správce front a adresářů protokolu do primárního uzlu RDRQM a dále veškeré samostatné zálohy úložišť certifikátů používaných správcem front.

b) Obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a ujistěte se, že vlastnictví souboru a oprávnění jsou zachována. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1c , může ho uživatel root použít následující příkaz k jeho obnovení:

```
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 a zkontrolujte, zda jsou vlastnictví souborů a oprávnění zachována. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1e , může jej uživatel root použít následující příkaz k jeho obnovení:

```
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` ve stanze `Log` , abyste určili adresář protokolu pro správce front RDQM.

Zkontrolujte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Například, možná budete muset aktualizovat následující cesty:

- Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
- Cesta k uživatelským procedurám, které jsou vyžadovány správcem front.
- Cesta k souborům načtení přepínače, je-li správce front koordinátorem transakcí XA.

e) Je-li správce front konfigurován tak, aby používal zachycení agenta MCA (AMS Message Channel Agent), zkopírujte úložiště klíčů AMS do nové instalace RDQM, poté zkontrolujte a aktualizujte konfiguraci. Úložiště klíčů musí být k dispozici v každém uzlu RDQM, takže pokud se nenachází v replikovaném systému souborů pro správce front, musí být místo toho zkopírován do každého uzlu. Další informace naleznete v tématu WebSphere Message Channel Agent (MCA) interception.

f) Ověřte, zda je správce front zobrazen příkazem **dspmq** a jeho stav je hlášen jako konec. Následující příklad zobrazuje ukázku výstupu pro správce front HA RDQM:

```
$ dspmq -o status -o ha

QMNAME(QM1) STATUS(Ended normally) HA(Replicated)
```

g) Verify that the restored queue manager data has been replicated to the secondary RDQM nodes by using the **rdqmstatus** command to display the status for the queue manager. Stav HA by měl být vykazována jako `Normal` na každém uzlu. Následující příklad zobrazuje ukázku výstupu pro správce front HA RDQM:

```
$ 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 RDRQM.

i) Připojte se ke správci front a aktualizujte hodnotu atributu správce front produktu SSLKEYR tak, aby určovala nové umístění úložiště certifikátů správce front. Při výchozím nastavení je hodnota tohoto atributu nastavena na *queue_manager_data_directory*/ssl/key. Úložiště certifikátů musí být umístěno ve stejném umístění v každém uzlu RDQM. Pokud se úložiště nenachází v replikovaném systému souborů pro správce front, musí být místo toho zkopírováno do každého uzlu.

j) Zkontrolujte definice objektů produktu 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 IP adresy použité kanály (atributLOCLADDR).
- Lokální IP adresy definované pro kanály příjemce klastru (atributCONNAME).
- Lokální IP adresy jsou definovány pro informační komunikační objekty (atributGRPADDR).
- Systémové cesty definované pro definice procesů a objektů služeb.

k) Zastavte a znovu spusťte správce front, aby se zajistilo, že změny budou platné.

l) Opakujte krok 3j pro vzdálené správce front a ekvivalentní nastavení pro aplikace, které se připojují k migrovanému správci front, včetně následujících:

- Názvy připojení kanálu (atributCONNAME).
- Pravidla ověřování kanálu, která omezují příchozí připojení ze správce front na základě jeho adresy IP nebo názvu hostitele.
- Definiční tabulky kanálu klienta (CCDT), nastavení názvu domény (DNS), směrování sítě nebo ekvivalentní informace o připojení.

m) Proveďte spravované překonání selhání správce front na každém uzlu RDQM, abyste se ujistili, že požadovaná konfigurace byla úspěšně zavedena, viz “Nastavení preferovaného umístění pro RDQM” na stránce 529.

Změna velikosti systému souborů pro správce front HA RDQM
Chcete-li změnit velikost systému souborů pro existujícího správce datových front s vysokou dostupností (RDS), zálohujete trvalá data, pak obnovte data do nově vytvořeného správce front RDQM, který má stejný název, ale systém souborů s jinou velikostí.

Informace o této úloze

Správci replikovaných datových front HA vyžadují vyhrazený logický svazek (systém souborů) a konfiguraci replikace disků a řízení HA. Tyto komponenty jsou konfigurovány pouze v případě, že je vytvořen nový správce front. Velikost systému souborů nelze změnit, protože byla vytvořena, protože musí mít stejnou velikost na každém uzlu. Chcete-li změnit velikost systému souborů pro existujícího replikovaného správce datových front (RDQM), můžete zálohovat jeho trvalá data a poté obnovit data do nově vytvořeného správce front RDQM, který má stejný název, ale systém souborů s jinou velikostí. Tento postup zachovává konfiguraci správce front, stav a trvalé zprávy v době vytvoření zálohy.

Postup

1. Zazálohujte existujícího správce front RDQM v primárním uzlu RDQM:
   a) Určete primární uzel RDRQM pro správce front. Informace o tom, jak určit primární uzel, najdete v tématu rdqmstatus (display RDRQM status) .
   b) Je-li správce front RDQM spuštěn v primárním uzlu RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .

c) Určete umístění datového adresáře správce front pomocí zobrazení konfiguračního souboru IBM MQ , `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`naleznete v tématu “IBM MQ konfigurační soubor mqs.ini” na stránce 82.

Vyhledejte sekci `QueueManager` pro správce front v souboru. Datový adresář správce front je hodnota klíče s názvem `DataPath`. Další informace o stanze `QueueManager` viz “QueueManager sekce souboru mqs.ini” na stránce 93.

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. Všimněte si posledního parametru příkazu, který je jediným znakem tečka (.):

```
tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
```

e) Určete umístění adresáře protokolu správce front pomocí zobrazení konfiguračního souboru správce front IBM MQ `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front qm.ini” na stránce 95.

Adresář protokolu správce front je definován jako hodnota klíče `LogPath` ve stanze Log. Informace o stanze viz “Sekce protokolu souboru qm.ini” na stránce 122.

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. Všimněte si posledního parametru příkazu, který je jediným znakem tečka (.):

```
tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
```

g) Odstraňte existujícího správce front RDQM.

2. Obnovte správce front s použitím systému souborů s požadovanou velikostí:

a) Vytvořte nového správce front RDQM se stejným názvem, jako má správce front, kterého jste zálohovali. Ujistěte se, že systém souborů alokovaný pro správce front RDQM o **crtmqm** je velikost, kterou vyžadujete, a je dostatečně velká, aby obsahovala data, primární protokoly a sekundární protokoly pro existujícího správce front a navíc některé další prostory pro budoucí expanzi. Informace o tom, jak vytvořit správce front RDQM, viz “Vytvoření agenta HA RDQM” na stránce 521.

b) Určete primární uzel RDRQM pro správce front. Informace o tom, jak určit primární uzel, najdete v tématu rdqmstatus (display RDRQM status).

c) Je-li správce front RDQM spuštěn v primárním uzlu RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .

d) Na primárním uzlu RQM určete nové umístění dat a adresářů protokolu pro správce front RDQM (použijte metody popsané v krocích 1c a 1e).

e) Na primárním uzlu RDQM odstraňte obsah adresářů správce front RDQM a adresářů protokolu, ale ne samotných adresářů.

f) Na primárním uzlu RDQM obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a ujistěte se, že vlastnictví souboru a oprávnění jsou zachována. Pokud byla záloha vytvořena pomocí vzorového příkazu **tar** v kroku 1d , může jej uživatel root použít následující příkaz k jeho obnovení:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

g) Na primárním uzlu RDQM obnovte zálohu adresáře protokolu správce front do prázdného adresáře protokolu pro nového správce front RDQM a ujistěte se, že vlastnictví souboru a oprávnění jsou zachována. Pokud byla záloha vytvořena pomocí vzorového příkazu **tar** v kroku 1f , může ho uživatel root použít následující příkaz k jeho obnovení:

```
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` ve stanze `Log` ,

abyste určili adresář protokolu pro nového správce front RDQM, který jste určili v kroku 2d. Zkontrolujte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Například, možná budete muset aktualizovat následující cesty:

- Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
- Cesta k uživatelským procedurám, které jsou vyžadovány správcem front.
- Cesta k souborům načtení přepínače, je-li správce front koordinátorem transakcí XA.

i) Ověřte, zda je správce front zobrazen příkazem **dspmq** a jeho stav je hlášen jako konec. Následující příklad zobrazuje ukázku výstupu pro správce front HA RDQM:

```
$ dspmq -o status -o ha
QMNAME(QM1) STATUS(Ended normally) HA(Replicated)
```

j) Verify that the restored queue manager data has been replicated to the secondary RDQM nodes by using the **rdqmstatus** command to display the status for the queue manager. Stav HA by měl být vykazována jako `Normal` na každém uzlu. Následující příklad zobrazuje ukázku výstupu pro správce front HA RDQM:

```
$ 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 RDRQM.

l) Proveďte spravované překonání selhání správce front na každém uzlu RDQM, abyste se ujistili, že požadovaná konfigurace byla úspěšně zavedena, viz “Nastavení preferovaného umístění pro RDQM” na stránce 529.

V 9.1.5 *Uložení stavu trvalé aplikace*

Informace o trvalém stavu můžete uložit spolu s dalšími daty správce front spolu s dalšími daty správce front.

Každý správce front produktu IBM MQ má vyhrazený systém souborů pro svůj trvalý stav, který obsahuje jak data fronty, tak i protokol zotavení. V konfiguraci RDQM je systém souborů zálohován logickým diskem, který je replikován mezi systémy Linux (uzly). Systém souborů obsahuje adresář `userdata` , který lze použít k ukládání trvalých stavových informací pro vaše aplikace. Takže, když se replikovaný správce datových front přesune na jiný uzel v konfiguraci RDQM, máte k dispozici kontext aplikace a kontext správce front. Viz Obsah adresáře v systémech Unix a Linux.

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

Adresář `userdata` má uživatele mqm a skupiny vlastníků a je to světově čitelný, takže uživatelé mohou k němu přistupovat, aniž by museli být ve skupině administrátorů produktu IBM MQ (to znamená mqm). Nemůžete upravit oprávnění k adresáři `userdata` , ale můžete v něm vytvořit obsah s libovolným vlastnictvím a oprávněními, které vyžadujete.

Během překonání selhání správce front RDQM je správce front ukončen a jeho systém souborů je uvolněn na svém aktuálním uzlu RDQM. Systém souborů se pak připojí a správce front se restartuje na jiném uzlu v konfiguraci RDQM. Systém souborů nelze odpojit, pokud má proces otevřený popisovač

pro jeden ze svých souborů. Chcete-li zajistit překonání selhání správce front, je-li systém souborů správce front nemůže být odpojen, je odeslán signál SIGTERM s otevřeným manipulátorem se signálem SIGTERM, pokud nejsou uvolněny otevřené manipulátory. Poté může být odeslán signál SIGTERM. 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, než bude systém souborů odpojen. Pokud není aplikace nebo proces konfigurován jako služba správce front nebo pokud dojde k nespravovanému překonání selhání, jako je například ztráta kvóty, je pravděpodobné, že signály budou odeslány k uvolnění systému souborů.

V 9.1.0 Linux *Nastavení preferovaného umístění pro RDQM*

Preferované umístění pro replikovaný správce datových front (RDMQM) identifikuje uzel, na kterém má být RDQM spuštěn, je-li tento uzel k dispozici.

Informace o této úloze

Preferované umístění je název uzlu, na kterém by měl Pacemaker spustit správce front, je-li skupina HA v normálním stavu (všechny uzly a připojení jsou k dispozici). Upřednostňované umístění je inicializováno na název primárního uzlu, když je správce front vytvořen. Můžete spustit příkazy k nastavení preferovaného umístění na libovolném ze tří uzlů. Musíte být uživatel, který patří do skupin `mqm` a `haclient` .

Procedura

- Chcete-li přiřadit lokální nebo určený uzel jako preferované umístění pro uvedeného správce front, zadejte následující příkaz:

  ```
  rdqmadm -p -m qmname [ -n nodename[,nodename  ]
  ```

  kde *qmname* je název RDQM, pro který uvádíte upřednostňované umístění, a *nodename* je volitelně název preferovaného uzlu.

  Je-li skupina HA v normálním stavu a preferované umístění není aktuální primární uzel, správce front se zastaví a znovu spustí na nové preferované umístění. Můžete uvést seznam názvů dvou uzlů oddělených čárkami, abyste přiřadili druhou předvolbu preferovaného umístění.
- Chcete-li vyčistit preferované umístění tak, aby se správce front nevracel automaticky do uzlu při obnově, zadejte následující příkaz:

  ```
  rdqmadm -p -m qmname -d
  ```

Související odkazy

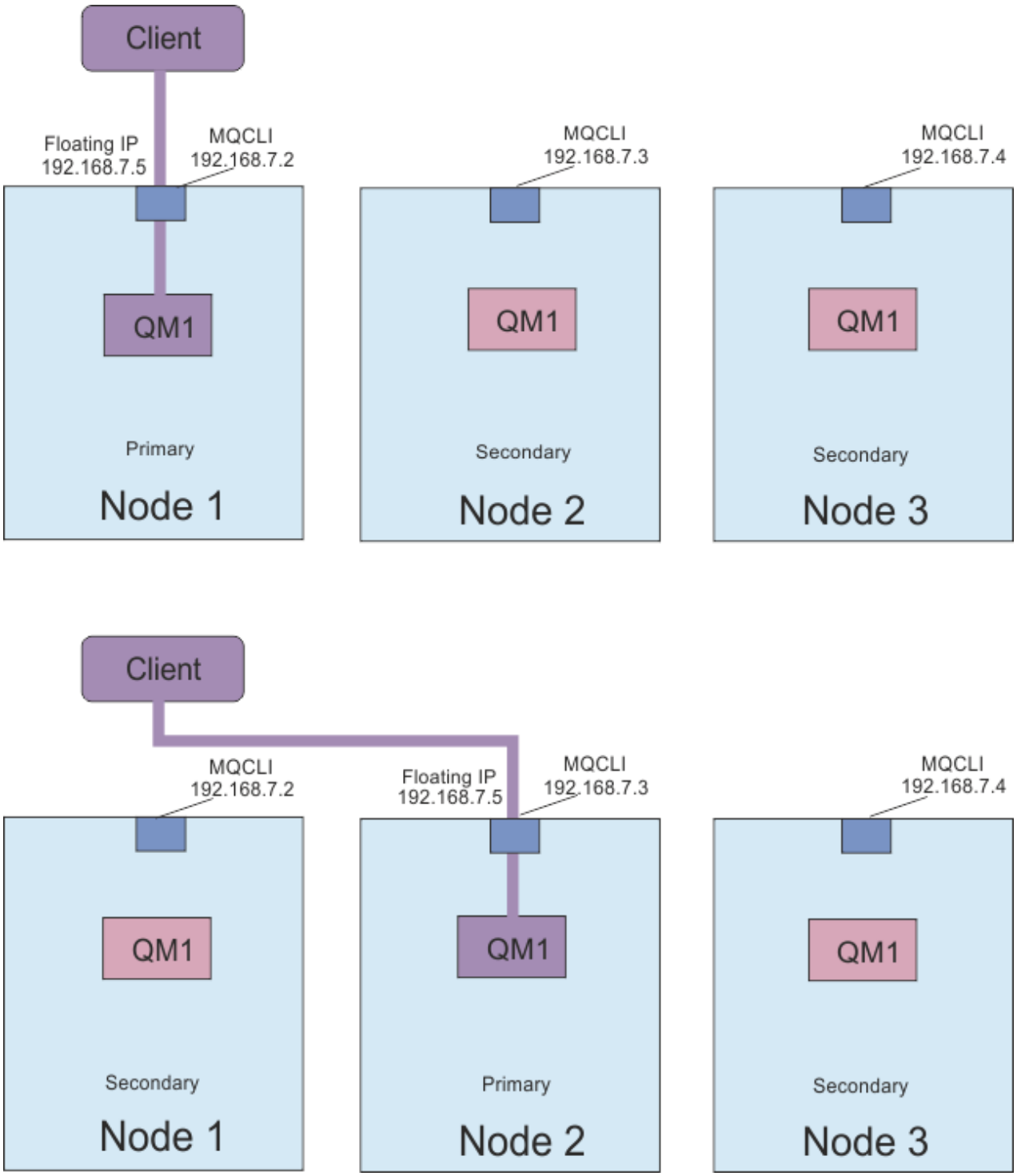
rdqmadm (spravovat replikovaný klastr správce datových front)

V 9.1.0 Linux *Vytvoření a odstranění plovoucí adresy IP*

Plovoucí adresa IP umožňuje klientovi použít stejnou adresu IP pro replikovaný správce datových front (RDQM) bez ohledu na to, který uzel ve skupině HA je spuštěný.

Informace o této úloze

Plovoucí adresu IP můžete vytvořit nebo odstranit pomocí příkazu **`rdqmint`** . Plovoucí adresa se váže k pojmenovanému fyzickému rozhraní na primárním uzlu pro RDQM. Pokud dojde k selhání RDRQM a primární uzel se stane primárním uzlem, bude plovoucí adresa IP svázána s rozhraním stejného názvu 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 83. Plovoucí adresa IP

Chcete-li spustit příkaz **rdqmint** , musíte být uživatelem ve skupinách `mqm` a `haclient` . Můžete vytvořit nebo odstranit plovoucí adresu IP na primárním uzlu pro RDQM, nebo buď ze sekundárních uzlů.

Poznámka: Nemůžete použít stejnou plovoucí adresu IP pro více modulů RDQM, plovoucí adresa IP pro každou aplikaci 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 platná adresa IPv4 , která ještě není definována na žádném zařízení, 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 MQCLI
```

- Chcete-li odstranit existující plovoucí adresu IP, zadejte následující příkaz:

```
rdqmint -m qmname -d
```

Související odkazy
rdqmint (přidání nebo odstranění plovoucí adresy IP pro RDQM)

V 9.1.0 Linux *Spuštění, zastavení a zobrazení stavu serveru HA RDQM*

Chcete-li spustit, zastavit a zobrazit aktuální stav replikovaného správce datových front (RDQM), použijte varianty standardních řídicích příkazů produktu IBM MQ .

Informace o této úloze

Musíte spustit příkazy, které spouštějí, zastavují a zobrazují aktuální stav replikovaného správce datových front (RDQM) jako uživatel, který patří do skupin `mqm` a `haclient` .

Chcete-li spustit a zastavit správce front v primárním uzlu pro daného správce front, je třeba spustit příkazy.

Procedura

- Chcete-li spustit RDQM, zadejte na primárním uzlu RDQM tento příkaz:

```
strmqm qmname
```

kde *qmname* je název RDQM, který chcete spustit.

RDQM je spuštěn a Pacemaker spustí správu RDQM. Chcete-li zadat jakékoli jiné volby `strmqm` , musíte zadat volbu `-ns` s volbou `strmqm` .

- Chcete-li zastavit RDQM, zadejte na primárním uzlu RDQM tento příkaz:

```
endmqm qmname
```

kde *qmname* je název RDQM, který chcete zastavit.

Pacemaker přestane spravovat RDQM, a pak se ukončí RDQM. Všechny ostatní parametry **endmqm** mohou být použity při zastavení RDQM.

- Chcete-li zobrazit stav RDQM, zadejte tento příkaz:

```
dspmq
```

Informace o stavu, které jsou výstupem, závisí na tom, zda jste spustili příkaz na primárním nebo sekundárním uzlu RDQM. Pokud se spustí na primárním uzlu, zobrazí se jedna z normálních stavových

zpráv vrácených serverem **dspmq** . Spustíte-li příkaz na sekundárním uzlu, zobrazí se stav `running elsewhere` . Je-li například **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 pokud je **dspmq** spuštěn uživatelem, který není `root` nebo členem skupiny `haclient` , pak se ohlásí stav `Unavailable` . Příklad:

```
QMNAME(RDQM8)               STATUS(Unavailable)
QMNAME(RDQM9)               STATUS(Unavailable)
QMNAME(RDQM7)               STATUS(Unavailable)
```

Můžete zadat příkaz **dspmq -o ha** (nebo **dspmq -o HA**), chcete-li zobrazit seznam správců front, o kterých uzel ví, a zda jsou to RDQMs, nebo ne, 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 (ukončit správce front)

strmqm (spuštění správce front)

V 9.1.0 Linux

Zobrazení stavu skupiny RDT a skupiny HA

Můžete zobrazit stav skupiny s vysokou dostupností a jednotlivých replikovaných správců datových front (RQMs).

Informace o této úloze

Příkaz **rdqmstatus** se používá k zobrazení stavu jednotlivých RDQM a skupiny HA jako celku.

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 stav uzlu a modulů RDQM, které jsou součástí konfigurace vysoké dostupnosti, postupujte takto:

  ```
  rdqmstatus
  ```

  Zobrazí se identifikace uzlu, na kterém jste spustili příkaz, a stav RDQM v konfiguraci vysoké dostupnosti, například:

  ```
  Node:                                   mqhavm07.exampleco.com

  Queue manager name:                     RDQM8
  Queue manager status:                   Running elsewhere
  HA current location:                    mqhavm08.exampleco.com

  Queue manager name:                     RDQM9
  Queue manager status:                   Running elsewhere
  HA current location:                    mqhavm09.exampleco.com

  Queue manager name:                     RDQM7
  Queue manager status:                   Running
  HA current location:                    This node
  ```

- Chcete-li zobrazit stav tří uzlů ve skupině HA, zadejte následující příkaz:

```
rdqmstatus -n
```

Je hlášen 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 určitého správce front ve všech uzlech ve skupině HA, 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 o stavu ostatních dvou uzlů z perspektivy aktuálního uzlu.

Následující tabulka shrnuje informace o aktuálním uzlu, který může být vrácen příkazem **rdqmstatus** pro RDQM.

Tabulka 33. Aktuální stav uzlu

Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Název uzlu	*NodeName*	Vždy zobrazit
Stav správce front	Spuštěno Spuštěno jinde Ukončeno Není k dispozici	Vždy zobrazit
CPU	*n.nn*%	Pouze zobrazeno, když má aktuální uzel primární roli (to znamená, že na tomto uzlu běží RDQM)
Paměť	*nnn*MB využito, *y.y*GB přiděleno	Pouze zobrazeno, když má aktuální uzel primární roli (to znamená, že na tomto uzlu běží RDQM)
Systém souborů správce front	*nnn*MB použito, *y.y*GB přiděleno [*z*%]	Pouze zobrazeno, když má aktuální uzel primární roli (to znamená, že na tomto uzlu běží RDQM)
Role HA	Primární sekundární neznámý	Vždy zobrazit
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 Odlišný stav pro každý vzdálený uzel (viz další tabulka pro jednotlivé stavy) Stejný stav pro oba vzdálené uzly (viz další tabulka pro všechny hodnoty)
Kontrola vysoké dostupnosti	Povoleno Zakázáno Neznámý	Vždy se zobrazí. Zobrazuje, zda je RDQM pod řízením Pacemaker

Tabulka 33. Aktuální stav uzlu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Preferované umístění HA	Není Tento uzel Neznámý *NodeName*	Vždy zobrazit
Plovoucí rozhraní IP HA	*název_rozhraní*	Vždy zobrazit
plovoucí adresa IP vysoké dostupnosti	*IPV4_address*	Vždy zobrazit

Následující tabulka shrnuje informace, které vrací příkaz **rdqmstatus** pro ostatní uzly ve skupině HA.

Tabulka 34. Stav jiného uzlu		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Název uzlu	*nodename*	Vždy zobrazit
Stav HA	Normální Probíhá synchronizace Vzdáleně nedostupné Nekonzistentní Pozastaveno Vzdálený uzel je v pohotovostním režimu Neznámý	Uzly jsou synchronizovány s ostatními Synchronizace se vzdáleným uzlem Nelze komunikovat se vzdáleným uzlem Není synchronizováno se vzdáleným uzlem a není synchronizováno Pozastavená replikace Vzdálený uzel je v pohotovostním režimu
Probíhá synchronizace HA	*n.n*%	Zobrazí se, když probíhá synchronizace, a příkaz spustit jako `root`
Odhadovaná doba synchronizace HA	*rrrr-mm-dd hh:mm:ss.nnn*	Zobrazí se, když probíhá synchronizace
Vysoká dostupnost nesynchronizovaných dat	*n*kB	Zobrazí se, když je vzdálený uzel nedostupný nebo nekonzistentní

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 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 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, když probíhá 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:                              Synchronization in progress
HA control:                             Enabled
HA current location:                    This node
HA preferred location:                  This node
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
```

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 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
```

Související odkazy

Linux rdqmstatus

V 9.1.0 Linux ***Náhrada vadného uzlu v konfiguraci vysoké dostupnosti***

Pokud jeden z uzlů ve skupině HA selže, můžete jej nahradit.

Informace o této úloze

Postup při nahrazení uzlu závisí na scénáři:

- Pokud nahrazujete uzel, který selhal, a uzel s identickou konfigurací, můžete uzel nahradit bez přerušení skupiny HA.
- Má-li nový uzel jinou konfiguraci, musíte ji odstranit a poté znovu sestavit skupinu HA. Nejprve můžete zálohovat správce front z uzlu, na kterém jsou spuštěni, a poté je obnovit poté, co jste znovu vytvořili skupinu s vysokou dostupností.

Procedura

- Je-li uzel nahrazení nakonfigurován tak, aby vypadal jako uzel, který selhal (stejný název hostitele, stejné IP adresy atd.), proveďte na novém uzlu následující kroky:
  a) Vytvořte soubor `rdqm.ini` , který se shoduje se soubory na jiných uzlech, a poté spusťte příkaz `rdqmadm -c` (viz “Definování klastru Pacemaker (HA group)” na stránce 518).
  b) Spuštěním příkazu `crtmqm -sxs qmanager` znovu vytvořte všechny replikované správce datových front (viz “Vytvoření agenta HA RDQM” na stránce 521).
- Má-li náhradní uzel jinou konfiguraci než uzel, který selhal, postupujte takto:
  a) V případě potřeby vytvořte zálohu pro správce front (viz “Zálohování a obnova dat správce front produktu IBM MQ” na stránce 601).
  b) Odstraňte replikované správce datových front z ostatních uzlů ve skupině s vysokou dostupností pomocí příkazu **dltmqm** (viz “Odstranění RDQM HA” na stránce 522).
  c) Zrušte konfiguraci klastru Pacemaker pomocí příkazu **rdqmadm -u** (viz “Odstranění klastru Pacemaker (skupina HA)” na stránce 521).
  d) Překonfigurujte klastr Pacemaker , včetně informací pro nový uzel, pomocí příkazu **rdqmadm -c** (viz “Definování klastru Pacemaker (HA group)” na stránce 518).
  e) Je-li to nezbytné (tj. pokud nemáte přístup SSH k ostatním uzlům), spusťte příkaz `crtmqm -sxs qmanager` k novému vytvoření každého replikovaného správce datových front na ostatních uzlech (viz “Vytvoření agenta HA RDQM” na stránce 521).
  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 produktu IBM MQ” na stránce 601).

V 9.1.0 MQ Adv. Linux zotavení z havárie RDQM

RDQM (replikovaný správce datových front) je k dispozici na podmnožině platforem Linux a může poskytnout řešení zotavení z havárie.

Podrobné informace najdete v tématu Sestavy o kompatibilitě softwarových produktů .

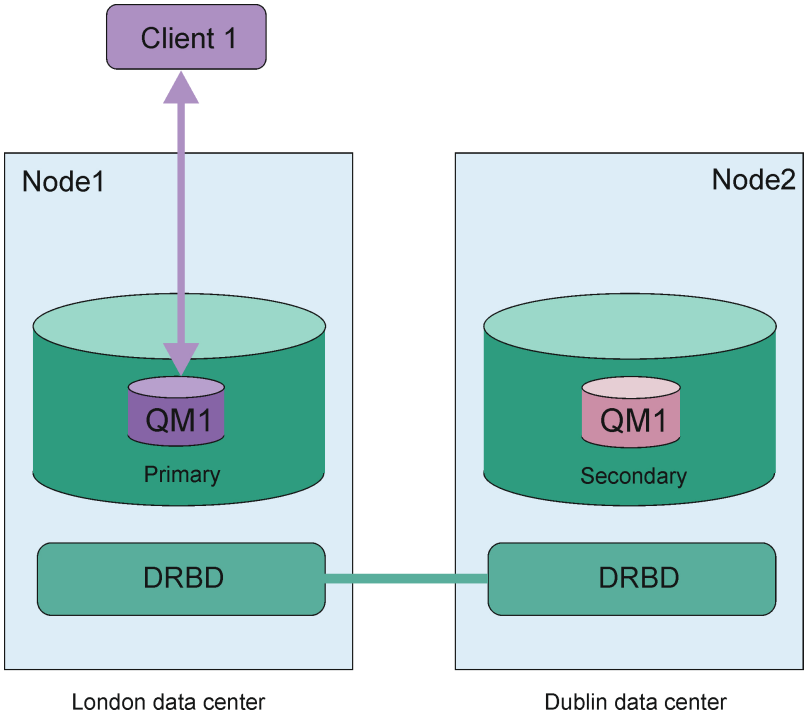
Můžete vytvořit primární instanci správce front pro zotavení z havárie spuštěnou na jednom serveru a sekundární instanci správce front na jiném serveru, který se chová jako uzel zotavení. Data jsou replikována mezi instancemi správce front. Pokud ztratíte primárního správce front, můžete ručně převést sekundární instanci do primární instance a spustit správce front a poté pokračovat v práci ze stejného místa. Správce front nelze spustit, dokud je v sekundární roli. Replikace dat mezi dvěma uzly se zpracovává pomocí DRBD.

Můžete zvolit synchronní a asynchronní replikaci dat mezi primárními a sekundárními správci front. Vyberete-li asynchronní volbu, budou operace jako IBM MQ PUT nebo GET dokončeny a vraťte se do aplikace před tím, než bude událost replikována do sekundárního správce front. Asynchronní replikace znamená, že v důsledku situace zotavení mohou být některá data systému zpráv ztracena. Sekundární správce front však bude v konzistentním stavu a může být spuštěn okamžitě, a to i v případě, že je spuštěn s mírně starší částí proudu zpráv.

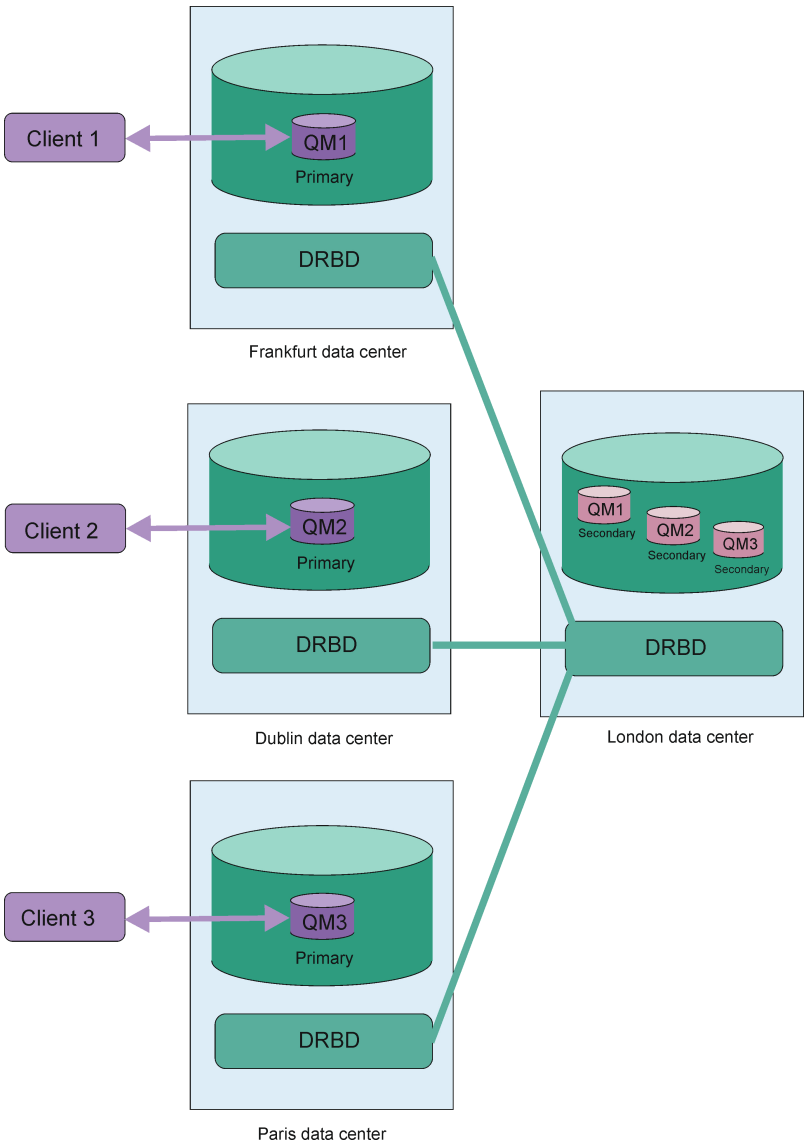
Nemůžete přidat zotavení z havárie do existujícího správce front, ačkoli můžete migrovat existujícího správce front, aby se stal správcem front RDQM (viz “Migrace správce front tak, aby se stal správcem

front DR RDQM” na stránce 543). Správce front nelze nakonfigurovat s oběma zotavením z havárie RDR a vysokou dostupností RQM.

Můžete mít několik párů správců front RDQM spuštěných na řadě různých serverů. Například, mohli byste mít primární správce front pro zotavení z havárie spuštěný na různých uzlech, zatímco všechny jejich sekundární správce front pro zotavení z havárie běží na stejném uzlu. Některé příklady konfigurací jsou ilustrovány v následujících diagramech.



Obrázek 84. Jedna dvojice RDQM



Obrázek 85. Sekundární správci front ve stejném uzlu

Replikace, synchronizace a snímky

Když jsou připojeny dva uzly v konfiguraci zotavení z havárie, všechny aktualizace trvalých dat pro správce front zotavení z havárie jsou přeneseny z primární instance správce front do sekundární instance. To se označuje jako **replikace**.

Dojde-li ke ztrátě síťového připojení mezi oběma uzly, budou sledovány změny trvalých dat pro primární instanci správce front. Když se obnoví připojení do sítě, použije se jiný proces k tomu, aby se sekundární instance dostala co nejrychleji do rychlosti. To se označuje jako **synchronizace**.

Když probíhá synchronizace, data na sekundární instanci jsou v nekonzistentním stavu. Je proveden **snímek** stavu dat sekundární správce front. Pokud dojde během synchronizace k selhání hlavního uzlu nebo k síťovému připojení, sekundární instance se vrátí k tomuto snímku a správce front může být spuštěn. Všechny aktualizace, které nastaly od doby selhání původní sítě, jsou však ztraceny.

Dělená data (rozdělovací mozek)

Konfigurace DR RDQM vyžadují akci uživatele po ztrátě primární instance správce front, aby povýšili a spustili sekundární instanci na uzlu nápravy. Je odpovědností toho, kdo (nebo co) povýší sekundární instanci, aby zajistil, že bývalý primární správce front je zastaven. Pokud původní primární server stále

běží, může zpracovávat zprávy a při obnově normální operace mají dvě instance správce front odlišné pohledy na data. To je známo jako rozdělený nebo štípkový stav mozku.

Zvažte následující situace:

- Uzel, v němž je spuštěn primární správce front, se zcela nezdaří. Povýšíte sekundární instanci, aby se stala primární; nemůžete provést akci k zastavení původní primární databáze, protože není spuštěna. Když je původní uzel opraven nebo vyměněn, bude správce front na tomto uzlu nejprve vytvořen sekundární a bude synchronizován s primárním správcem front v uzlu zotavení. Role těchto dvou správců front jsou poté obrácené a normální operace jsou znovu doporučeny. Jediná potenciální ztráta dat v této situaci jsou jakákoli data, která primární databáze nedokončila replikace na sekundárním serveru, než došlo k selhání uzlu.
- Došlo k selhání sítě, které ovlivňuje propojení replikace mezi uzly, na kterých jsou spuštěny primární a sekundární instance správce front. V této situaci musíte zajistit zastavení původní primární databáze před tím, než budete podporovat sekundární úroveň. Má-li původní primární server stále ještě další připojitelnost k síti, máte ve stejnou dobu spuštěny dvě primární instance a mohou se nahromadí data s rozdělením na oblasti. (Pokud replikační odkaz pracuje, nelze povýšit sekundárního správce front, je-li primární instance stále spuštěna, příkaz selže.)
- Na uzlu, na kterém je spuštěna primární instance správce front, došlo k úplnému selhání sítě. Opět musíte zajistit zastavení primární instance před tím, než budete podporovat sekundární instanci. Je-li předchozí primární uzel stále spuštěn při obnově sítě, budou existovat dvě primární instance a znovu budou rozdělena data rozdělená na oblasti.

Provedete-li spravované překonání selhání, neměl by být pro instance správce front zobrazen stav DR `partitioned` . Spravované překonání selhání ukončí správce front v primárním uzlu a poté spustí správce front na uzlu zotavení poté, co byla data plně replikována. Rozdělený stav není očekáván, protože je správce front ukončen a data jsou synchronizována mezi uzly před jejím spuštěním na uzlu nápravy. Je-li správce front spuštěn v uzlu zotavení, došlo-li ke ztrátě konektivity mezi uzly, pak je pravděpodobné, že při ztrátě připojení je správce front aktivní v hlavním uzlu. V tomto scénáři se předpokládá, že stav rozdělení na oblasti bude hlášen po obnovení konektivity, protože data správce front nebyla synchronizována. Pokud nastane stav rozděleném na logické oblasti, budete možná muset prozkoumat dvě datové sady a učinit informované rozhodnutí o tom, co nastavit. Viz téma “Řešení problému rozděleného na oblasti (rozdělení mozku) v DR RDQM” na stránce 556.

V 9.1.0 Linux

Požadavky pro řešení DR RDQM

Před konfigurací dvojice správce front pro zotavení z havárie (DR) musíte splnit požadavky na řadu požadavků.

Systémové požadavky

Před konfigurací DR DR je třeba dokončit některé konfigurace na každém ze serverů, které jsou hostiteli správců front DR RDR.

- Každý uzel vyžaduje skupinu disků s názvem `drbdpool`. Úložiště pro každého replikovaného správce datových front zotavení z havárie (DR RDQM) je alokováno jako dva samostatné logické svazky na správce front z této skupiny disků. (Každý správce front vyžaduje dva logické svazky, aby podporoval opětovné vrácení na operaci snímku, takže každý DR RDQM je přidělen právě přes dvojnásobek úložiště, které určíte, když jej vytvoříte.) Pro nejlepší výkon by tato skupina disků měla být tvořena jedním nebo více fyzickými disky, které odpovídají interním diskovým jednotkám (pokud možno SSD).
- Poté, co jste vytvořili skupinu disků `drbdpool` , nedělejte s ní nic jiného. Produkt IBM MQ spravuje logické svazky vytvořené v produktu `drbdpoola` jak a kde jsou připojeny.
- Každý uzel vyžaduje rozhraní, které se používá pro replikaci dat. To by mělo mít dostatečnou šířku pásma pro podporu požadavků replikace vzhledem k očekávané zátěži všech replikovaných správců datových front.

  Pro maximální odolnost proti poruchám by toto rozhraní mělo být nezávislé karty síťového rozhraní (NIC).

- DRBD vyžaduje, aby každý uzel použitý pro RDQM měl platný internetový název hostitele (hodnota vrácená produktem `uname -n`), jak je definováno v RFC 952, změněném RFC 1123.
- Je-li mezi uzly používanými pro DR RDQM brána firewall, musí brána firewall povolit provoz mezi uzly na portech, které se používají pro replikaci.
- Pokud systém používá SELinux v jiném režimu, než je permissive, musíte spustit tento příkaz:

```
semanage permissive -a drbd_t
```

Síťové požadavky

Doporučuje se vyhledat uzly použité pro zotavení z havárie v různých datových centrech.

Měli byste si být vědomi následujících omezení:

- Výkon se rychle zhoršuje se zvyšující se latencí mezi datovými centry. IBM bude podporovat latenci až 5 ms pro synchronní replikaci a 50 ms pro asynchronní replikaci.
- Data odeslaná přes replikační odkaz se nevztahují na žádné další šifrování, které by mohlo být na místě, které by mohlo být použito při použití serveru IBM MQ AMS.
- Konfigurace správce front RDQM pro zotavení z havárie je v důsledku požadavku na replikaci dat mezi dvěma uzly RDQM. Synchronní replikace způsobí větší režii než asynchronní replikace. Je-li použita synchronní replikace, operace I/O disku jsou blokovány, dokud nejsou data zapsána do obou uzlů. Je-li použita asynchronní replikace, musí být data zapsána pouze do primárního uzlu, a teprve pak může zpracování pokračovat.

Požadavky na uživatele pro práci se správci front

Chcete-li vytvořit, odstranit nebo nakonfigurovat replikované správce datových front (RQMs), musíte být buď uživatel root, nebo mít ID uživatele patřící do skupiny `mqm` , která má udělené oprávnění sudo pro následující příkazy:

- **`crtmqm`**
- **`dltmqm`**
- **`rdqmdr`**

Uživatel, který patří do skupiny `mqm` , může zobrazit stav a stav RDR RDQM pomocí následujících příkazů:

- **`dspmq`**
- **`rdqmstatus`**

V 9.1.0 Linux

Vytvoření zotavení z havárie RDQM

Pomocí příkazu **`crtmqm`** můžete vytvořit replikovaný správce datových front (RDRQM), který bude sloužit jako primární nebo sekundární v konfiguraci zotavení z havárie.

Informace o této úloze

Pokud uživatel může použít příkaz sudo, můžete vytvořit replikovaný správce datových front (RDQM) jako uživatel ve skupině `mqm` . Jinak musíte vytvořit RDQM jako kořen.

Musíte vytvořit primárního správce front DR RDQM na jednom uzlu. Poté je třeba vytvořit sekundární instanci stejného správce front v jiném uzlu. Primární a sekundární instance musí mít stejný název a musí být přiděleny stejné množství úložiště.

Procedura

- Chcete-li vytvořit primární DR RDQM:

  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. Výchozím nastavením je asynchronní replikace.

-rl *Lokální_IP*
Určuje adresu IP lokálního systému, 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 *obnovy_zotavení*
Určuje název systému, který je hostitelem sekundární instance správce front. Název je taková hodnota, která je vrácena, pokud na daném serveru spustíte produkt `uname -n` . Na tomto serveru je třeba explicitně vytvořit sekundárního správce front.

-rp *Port*
Uvádí port, který se má použít pro replikaci DR.

other_crtm_qm_options
Volitelně můžete zadat jednu nebo více z těchto obecných voleb obslužného programu **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 svazku, který je vytvořen ve skupině svazků drbdpool. Je také vytvořen jiný logický svazek této velikosti, který podporuje návrat k operaci snímku, takže celkové úložiště pro DR RDQM je právě více než dvojnásobek, které je zde uvedeno.

QMNAME
Určuje název replikovaného správce datových front. V názvu jsou rozlišována velká a malá písmena.

Po dokončení příkazu se výstupem příkazu vypíše příkaz, který pro vytvoření sekundární instance správce front vyžaduje zadání tp na sekundárním uzlu. Příkaz **rdqmdr** můžete také použít na svém

primárním uzlu, abyste načetli příkaz **crtmqm** , který musíte spustit na sekundárním uzlu, abyste mohli vytvořit sekundárního správce front, viz “Správa primárních a sekundárních charakteristik RDQMs DR” na stránce 549.

- Chcete-li vytvořit sekundární RDR DR:

  a) Zadejte následující příkaz na uzlu, který má hostovat sekundární instance 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 *Lokální_IP*
  Určuje adresu IP lokálního systému, která má být použita pro replikaci DR tohoto správce front.

  -ri *Primární_IP*
  Určuje adresu IP rozhraní používaného pro replikaci na serveru, který je hostitelem primární instance správce front.

  -rn *Primární_název*
  Určuje název systému, který je hostitelem primární instance správce front. Název je taková hodnota, která je vrácena, pokud na daném serveru spustíte produkt `uname -n` .

  -rp *Port*
  Uvádí port, který se má použít pro replikaci DR.

  other_crtm_qm_options
  Volitelně můžete zadat jednu nebo více z těchto obecných voleb obslužného programu **crtmqm** :

  – `-z`

  -fs *velikost*
  Určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického svazku, který je vytvořen ve skupině svazků drbdpool. Pokud jste při vytváření primárního správce front zadali jinou než výchozí velikost, je třeba zde zadat stejnou hodnotu.

  QMNAME
  Určuje název replikovaného správce datových front. Musí to být stejné jako název, který jste zadali pro primární instanci správce front. Všimněte si, že název rozlišuje velikost písmen.

Jak pokračovat dále

Po vytvoření primární a sekundární instance správce front je nutné zkontrolovat správnost stavu obou uzlů. Použijte příkaz **rdqmstatus** na obou uzlech. Uzly by měly zobrazovat normální stav, jak je popsáno v tématu “Zobrazení stavu DR RDQM” na stránce 550. Pokud tento stav nezobrazujete, odstraňte sekundární instanci a znovu ji vytvořte, přičemž je třeba dbát na správné argumenty.

Související odkazy

crtmqm

V 9.1.0 Linux *Odstranění DR RDQM*

Příkaz **dltmqm** se používá k odstranění replikovaného správce datových front (RDQM) pro zotavení z havárie.

Informace o této úloze

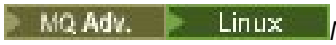
Musíte spustit příkaz k odstranění RDMQM na primárním i sekundárním uzlu RDQM. RDQM musí být ukončen první. Příkaz můžete spustit jako uživatel mqm, pokud má tento uživatel potřebná oprávnění k příkazu sudo. Jinak musíte spustit příkaz jako uživatel root.

Procedura

- Chcete-li odstranit RDR RDR, zadejte následující příkaz:

```
dltmqm RDQM_name
```

Související odkazy
dltmqm



Migrace správce front tak, aby se stal správcem front DR RDQM

Existující správce front můžete migrovat tak, aby se stal replikovaným správcem front pro zotavení z havárie (DR) tak, že zálohoval její trvalá data a poté obnovil data do nově vytvořeného správce front RDQM, který má stejný název.

Informace o této úloze

Replikovaný správce datových front replikace dat vyžaduje vyhrazený logický svazek (systém souborů) a konfiguraci replikace disků. Tyto komponenty jsou konfigurovány pouze v případě, že je vytvořen nový správce front. Existující správce front lze migrovat tak, aby používal RDQM tak, že zálohuje trvalá data a poté obnoví data do nově vytvořeného správce front RDQM, který má stejný název. Tento postup zachovává konfiguraci správce front, stav a trvalé zprávy v době vytvoření zálohy.

Poznámka: Migraci správce front můžete provést pouze z verze produktu IBM MQ , která je stejná nebo nižší než verze, na které je nainstalován produkt RDQM. Operační systém a architektura musí být také stejné. Jinak je třeba na cílové platformě vytvořit nového správce front, viz téma Přesun správce front do jiného operačního systému.

Před migrací správce front byste měli splnit následující podmínky:

- Vyhodnoťte vaše požadavky na zotavení z havárie a zobrazte téma “zotavení z havárie RDQM” na stránce 536.
- Zkontrolujte aplikace a správce front, kteří se připojují ke správci front. Zvažte změny nezbytné pro směrování připojení k uzlu RDQM, kde je spuštěn správce front.
- Zajistěte nebo identifikujte existující uzly RDQM pro zvolenou konfiguraci. Informace o systémových požadavcích pro RDQM viz “Požadavky pro řešení DR RDQM” na stránce 539.
- Nainstalujte produkt IBM MQ Advanced, který obsahuje funkci RDQM, na každém uzlu.
- Volitelně ověřte konfiguraci RDQM pomocí správce testovací fronty, který lze poté odstranit. Testování konfigurace se doporučuje identifikovat a vyřešit případné problémy před migrací správce front.
- Zkontrolujte konfiguraci zabezpečení správce front a poté replikujte požadované lokální uživatele a skupiny do každého uzlu RDQM.
- Zkontrolujte správce front a konfiguraci kanálu a zjistěte, zda se používají uživatelské procedury rozhraní API, ukončení kanálu nebo ukončení převodu dat. Nainstalujte požadované uživatelské procedury na každý uzel RDQM.
- Zkontrolujte všechny definované služby správce front, pak nainstalujte a nakonfigurujte požadované procesy na každém uzlu RDQM.

Postup

1. Vytvořte zálohu stávajícího správce front:

a) Zastavte existujícího správce front zadáním příkazu wait shutdown `endmqm -w`nebo příkazem okamžitého ukončení práce systému `endmqm -i`. Tento krok je důležitý pro zajištění konzistence dat v záloze.

b) Určete umístění datového adresáře správce front pomocí zobrazení konfiguračního souboru IBM MQ , `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`naleznete v tématu “IBM MQ konfigurační soubor mqs.ini” na stránce 82.

Vyhledejte sekci `QueueManager` pro správce front v souboru. Pokud stanza obsahuje klíč s názvem `DataPath` , pak jeho hodnota je datový adresář správce front. Pokud klíč neexistuje, může být datový adresář správce front určen pomocí hodnot klíčů `Prefix` a `Directory` . Datový adresář správce front je zřetězením těchto hodnot ve tvaru *předpona*/qmgrs/*adresář*. Další informace o sekci QueueManager viz “QueueManager sekce souboru mqs.ini” na stránce 93.

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, který je jediným obdobím (tečka):

```
tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
```

d) Určete umístění adresáře protokolu správce front pomocí zobrazení konfiguračního souboru správce front IBM MQ `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front qm.ini” na stránce 95.

Adresář protokolu správce front je definován jako hodnota klíče `LogPath` ve stanze `Log` . Informace o stanze viz “Sekce protokolu souboru qm.ini” na stránce 122.

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, který je jediným obdobím (tečka):

```
tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
```

f) Vytvořte zálohu všech úložišť certifikátů používaných správcem front, nejsou-li umístěny v datovém adresáři správce front. Ujistěte se, že je zálohovaný jak soubor databáze klíčů, tak soubor pro uložení hesla. Informace o úložišti klíčů správce front najdete v tématu Úložiště klíčů SSL/TLS a Nalezení úložiště klíčů pro správce front. Informace o umístění úložiště klíčů AMS, je-li správce front konfigurován pro použití zachycování agenta MCA (AMS Message Channel Agent), najdete v tématu WebSphere Message Channel Agent (MCA) interception.

g) Existující správce front již není požadován, takže jej lze odstranit. Je-li to možné, měli byste odstranit pouze existujícího správce front poté, co byl úspěšně obnoven na cílovém systému. Odložení odstranění zajišťuje, že správce front může být restartován, pokud se proces migrace nedokončí úspěšně.

Poznámka: Pokud odložíte odstranění existujícího správce front, nerestartujte jej. Je důležité, aby správce front byl ukončen, protože během migrace byly ztraceny další změny jeho konfigurace nebo stavu.

2. Připravte primární uzel RDQM:

a) Vytvořte nového správce front RDQM se stejným názvem, jako má správce front, kterého jste zálohovali. Ujistěte se, že systém souborů alokovaný pro správce front RDQM produktem **`crtmqm`** je dostatečně velký, aby obsahoval data, primární protokoly a sekundární protokoly pro existujícího správce front a navíc některé další prostory pro budoucí rozšíření. Informace o tom, jak vytvořit správce front RDQM, viz “Vytvoření zotavení z havárie RDQM” na stránce 540.

b) Určete primární uzel RDRQM pro správce front. Informace o tom, jak určit primární uzel, najdete v tématu rdqmstatus (display RDRQM status).

c) Je-li správce front RDQM spuštěn v primárním uzlu RDQM, zastavte jej pomocí příkazu `endmqm -w` nebo `endmqm -i` .

d) Určete umístění dat a adresářů protokolu pro správce front RDQM (použijte metody popsané v krocích 1b a 1d).

e) Odstraňte obsah dat správce front RDQM a adresářů protokolu, ale ne adresáře samotných.

3. Obnovte správce front v primárním uzlu RDQM:
   a) Zkopírujte zálohy dat správce front a adresářů protokolu do primárního uzlu RDRQM a dále veškeré samostatné zálohy úložišť certifikátů používaných správcem front.
   b) Obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a ujistěte se, že vlastnictví souboru a oprávnění jsou zachována. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1c , může ho uživatel root použít následující příkaz k jeho obnovení:

      ```
      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 a zkontrolujte, zda jsou vlastnictví souborů a oprávnění zachována. Pokud byla záloha vytvořena pomocí ukázkového příkazu tar v kroku 1e , může jej uživatel root použít následující příkaz k jeho obnovení:

      ```
      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` ve stanze `Log` , abyste určili adresář protokolu pro správce front RDQM.

      Zkontrolujte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Například, možná budete muset aktualizovat následující cesty:

      - Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
      - Cesta k uživatelským procedurám, které jsou vyžadovány správcem front.
      - Cesta k souborům načtení přepínače, je-li správce front koordinátorem transakcí XA.

   e) Je-li správce front konfigurován tak, aby používal zachycení agenta MCA (AMS Message Channel Agent), zkopírujte úložiště klíčů AMS do nové instalace RDQM, poté zkontrolujte a aktualizujte konfiguraci. Úložiště klíčů musí být k dispozici v každém uzlu RDQM, takže pokud se nenachází v replikovaném systému souborů pro správce front, musí být místo toho zkopírován do každého uzlu. Další informace naleznete v tématu WebSphere Message Channel Agent (MCA) interception.
   f) Ověřte, zda je správce front zobrazen příkazem **dspmq** a jeho stav je hlášen jako konec. Následující příklad zobrazuje ukázku výstupu pro správce front DR RDQM:

      ```
      $ dspmq -o status -o dr

      QMNAME(QM1) STATUS(Ended normally) DRROLE(Primary)
      ```

   g) Verify that the restored queue manager data has been replicated to the secondary RDQM nodes by using the **rdqmstatus** command to display the status for the queue manager. Stav DR by měl být ohlášen jako `Normal` na každém uzlu. Následující příklad zobrazuje ukázku výstupu pro správce front DR RDQM:

      ```
      $ 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 RDRQM.
   i) Připojte se ke správci front a aktualizujte hodnotu atributu správce front produktu SSLKEYR tak, aby určovala nové umístění úložiště certifikátů správce front. Při výchozím nastavení je hodnota tohoto atributu nastavena na *queue_manager_data_directory*`/ssl/key`. Úložiště certifikátů musí být umístěno ve stejném umístění v každém uzlu RDQM. Pokud se úložiště nenachází v replikovaném systému souborů pro správce front, musí být místo toho zkopírováno do každého uzlu.

j) Zkontrolujte definice objektů produktu 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 IP adresy použité kanály (atributLOCLADDR).
- Lokální IP adresy definované pro kanály příjemce klastru (atributCONNAME).
- Lokální IP adresy jsou definovány pro informační komunikační objekty (atributGRPADDR).
- Systémové cesty definované pro definice procesů a objektů služeb.

k) Zastavte a znovu spusťte správce front, aby se zajistilo, že změny budou platné.

l) Opakujte krok 3j pro vzdálené správce front a ekvivalentní nastavení pro aplikace, které se připojují k migrovanému správci front, včetně následujících:

- Názvy připojení kanálu (atributCONNAME).
- Pravidla ověřování kanálu, která omezují příchozí připojení ze správce front na základě jeho adresy IP nebo názvu hostitele.
- Definiční tabulky kanálu klienta (CCDT), nastavení názvu domény (DNS), směrování sítě nebo ekvivalentní informace o připojení.

m) Proveďte spravované překonání selhání správce front na každém uzlu RDQM, abyste se ujistili, že požadovaná konfigurace byla úspěšně zavedena, viz “Přepnutí na uzel nápravy” na stránce 553.

Změna velikosti systému souborů pro správce front DR RDQM
Chcete-li změnit velikost systému souborů pro existujícího správce datových front zotavení z havárie (DR), zálohujete jeho trvalá data, pak obnovte data do nově vytvořeného správce front RDQM, který má stejný název, ale systém souborů s jinou velikostí.

Informace o této úloze

Replikovaný správce datových front DR vyžaduje vyhrazený logický svazek (systém souborů) a konfiguraci replikace disků. Tyto komponenty jsou konfigurovány pouze v případě, že je vytvořen nový správce front. Velikost systému souborů nelze změnit, protože byla vytvořena, protože musí mít stejnou velikost na každém uzlu. Chcete-li změnit velikost systému souborů pro existujícího replikovaného správce datových front (RDQM), můžete zálohovat jeho trvalá data a poté obnovit data do nově vytvořeného správce front RDQM, který má stejný název, ale systém souborů s jinou velikostí. Tento postup zachovává konfiguraci správce front, stav a trvalé zprávy v době vytvoření zálohy.

Postup

1. Zazálohujte existujícího správce front RDQM v primárním uzlu RDQM:
   a) Určete primární uzel RDRQM pro správce front. Informace o tom, jak určit primární uzel, najdete v tématu rdqmstatus (display RDRQM status) .
   b) Je-li správce front RDQM spuštěn v primárním uzlu RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .
   c) Určete umístění datového adresáře správce front pomocí zobrazení konfiguračního souboru IBM MQ , `mqs.ini`. V systému Linuxje tento soubor umístěn v adresáři `/var/mqm` . Další informace o produktu `mqs.ini`naleznete v tématu “IBM MQ konfigurační soubor mqs.ini” na stránce 82.

      Vyhledejte sekci `QueueManager` pro správce front v souboru. Datový adresář správce front je hodnota klíče s názvem `DataPath`. Další informace o stanze `QueueManager` viz “QueueManager sekce souboru mqs.ini” na stránce 93.
   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. Všimněte si posledního parametru příkazu, který je jediným znakem tečka (.):

```
tar -cvzf qm-data.tar.gz -C queue_manager_data_dir .
```

e) Určete umístění adresáře protokolu správce front pomocí zobrazení konfiguračního souboru správce front IBM MQ `qm.ini`. Tento soubor je umístěn v datovém adresáři správce front. Další informace o souboru viz “Konfigurační soubory správce front qm.ini” na stránce 95.

Adresář protokolu správce front je definován jako hodnota klíče `LogPath` ve stanze `Log`. Informace o stanze viz “Sekce protokolu souboru qm.ini” na stránce 122.

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. Všimněte si posledního parametru příkazu, který je jediným znakem tečka (.):

```
tar -cvzf qm-log.tar.gz -C queue_manager_log_dir .
```

g) Odstraňte existujícího správce front RDQM.

2. Obnovte správce front s použitím systému souborů s požadovanou velikostí:

a) Vytvořte nového správce front RDQM se stejným názvem, jako má správce front, kterého jste zálohovali. Ujistěte se, že systém souborů alokovaný pro správce front RDQM o **crtmqm** je velikost, kterou vyžadujete, a je dostatečně velká, aby obsahovala data, primární protokoly a sekundární protokoly pro existujícího správce front a navíc některé další prostory pro budoucí expanzi. Informace o tom, jak vytvořit správce front RDQM, viz “Vytvoření zotavení z havárie RDQM” na stránce 540.

b) Určete primární uzel RDRQM pro správce front. Informace o tom, jak určit primární uzel, najdete v tématu rdqmstatus (display RDRQM status).

c) Je-li správce front RDQM spuštěn v primárním uzlu RDQM, zastavte jej pomocí příkazu **endmqm -w** nebo **endmqm -i** .

d) Na primárním uzlu RQM určete nové umístění dat a adresářů protokolu pro správce front RDQM (použijte metody popsané v krocích 1c a 1e).

e) Na primárním uzlu RDQM odstraňte obsah adresářů správce front RDQM a adresářů protokolu, ale ne samotných adresářů.

f) Na primárním uzlu RDQM obnovte zálohu datového adresáře správce front do prázdného datového adresáře pro nového správce front RDQM a ujistěte se, že vlastnictví souboru a oprávnění jsou zachována. Pokud byla záloha vytvořena pomocí vzorového příkazu **tar** v kroku 1d , může jej uživatel root použít následující příkaz k jeho obnovení:

```
tar -xvzpf qm-data.tar.gz -C queue_manager_data_dir
```

g) Na primárním uzlu RDQM obnovte zálohu adresáře protokolu správce front do prázdného adresáře protokolu pro nového správce front RDQM a ujistěte se, že vlastnictví souboru a oprávnění jsou zachována. Pokud byla záloha vytvořena pomocí vzorového příkazu **tar** v kroku 1f , může ho uživatel root použít následující příkaz k jeho obnovení:

```
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` ve stanze `Log` , abyste určili adresář protokolu pro nového správce front RDQM, který jste určili v kroku 2d. Zkontrolujte další cesty k souborům, které jsou definovány v konfiguračním souboru, a v případě potřeby je aktualizujte. Například, možná budete muset aktualizovat následující cesty:

- Cesta k souborům protokolu chyb, které jsou generovány službami diagnostických zpráv.
- Cesta k uživatelským procedurám, které jsou vyžadovány správcem front.
- Cesta k souborům načtení přepínače, je-li správce front koordinátorem transakcí XA.

i) Ověřte, zda je správce front zobrazen příkazem **dspmq** , a jeho stav je ohlášen jako `ended`. Následující příklad zobrazuje ukázku výstupu pro správce front DR RDQM:

```
$ dspmq -o status -o dr
QMNAME(QM1) STATUS(Ended normally) DR(Primary)
```

j) Verify that the restored queue manager data has been replicated to the secondary RDQM node by using the **rdqmstatus** command to display the status for the queue manager. Stav DR by měl být ohlášen jako `Normal` na každém uzlu. Následující příklad zobrazuje ukázku výstupu pro správce front DR RDQM 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 zobrazuje ukázku výstupu pro správce front DR RDQM 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 RDRQM.

l) Proveďte přepnutí správce front na uzel nápravy, abyste se ujistili, že požadovaná konfigurace byla úspěšně zavedena, viz “Přepnutí na uzel nápravy” na stránce 553.

V 9.1.5 *Uložení stavu trvalé aplikace*

Informace o trvalém stavu můžete uložit spolu s dalšími daty správce front spolu s dalšími daty správce front.

Každý správce front produktu IBM MQ má vyhrazený systém souborů pro svůj trvalý stav, který obsahuje jak data fronty, tak i protokol zotavení. V konfiguraci RDQM je systém souborů zálohován logickým diskem, který je replikován mezi systémy Linux (uzly). Systém souborů obsahuje adresář `userdata` , který lze použít k ukládání trvalých stavových informací pro vaše aplikace. Takže, když se replikovaný správce datových front přesune na jiný uzel v konfiguraci RDQM, máte k dispozici kontext aplikace a kontext správce front. Viz Obsah adresáře v systémech Unix a Linux.

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

Adresář `userdata` má uživatele mqm a skupiny vlastníků a je to světově čitelný, takže uživatelé mohou k němu přistupovat, aniž by museli být ve skupině administrátorů produktu IBM MQ (to znamená mqm). Nemůžete upravit oprávnění k adresáři `userdata` , ale můžete v něm vytvořit obsah s libovolným vlastnictvím a oprávněními, které vyžadujete.

Během překonání selhání správce front RDQM je správce front ukončen a jeho systém souborů je uvolněn na svém aktuálním uzlu RDQM. Systém souborů se pak připojí a správce front se restartuje na jiném uzlu v konfiguraci RDQM. Systém souborů nelze odpojit, pokud má proces otevřený popisovač pro jeden ze svých souborů. Chcete-li zajistit překonání selhání správce front, je-li systém souborů správce front nemůže být odpojen, je odeslán signál SIGTERM s otevřeným manipulátorem se signálem SIGTERM, pokud nejsou uvolněny otevřené manipulátory. Poté může být odeslán signál SIGTERM. 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, než bude systém souborů odpojen. Pokud není aplikace nebo proces konfigurován jako služba správce front nebo pokud dojde k nespravovanému překonání selhání, jako je například ztráta kvóty, je pravděpodobné, že signály budou odeslány k uvolnění systému souborů.

V 9.1.0 Linux *Správa primárních a sekundárních charakteristik RDQMs DR*

Sekundární správce datových front replikovaných dat zotavení z havárie (DR RDQM) můžete změnit na primární DR RDR. Primární instanci můžete také změnit na sekundární instanci.

Informace o této úloze

Příkaz **rdqmdr** se používá ke změně sekundární instance RDQM do primární instance. Možná budete muset dokončit tuto akci, pokud ztratíte primární instanci z nějakého důvodu. Poté můžete spustit správce front a pokračovat jeho spuštěním na uzlu zotavení.

Chcete-li změnit primární instanci RDMQM do sekundární instance, použijte také příkaz **rdqmdr** . Možná budete muset dokončit tuto akci, například, pokud jste rekonfigurovali svůj systém.

K získání přesného příkazu, který potřebujete k vytvoření sekundární instance tohoto správce front na uzlu obnovy, můžete také použít program **rdqmdr** v primárním správci front.

Příkaz **rdqmdr** můžete použít jako uživatele ve skupině `mqm` , může-li uživatel použít příkaz sudo. Jinak musíte být přihlášeni jako uživatel root.

Procedura

- Chcete-li změnit sekundární instanci DR RDQM na primární instanci, zadejte tento příkaz:

  ```
  rdqmdr -m QMname -p
  ```

  Tento příkaz selže, je-li primární instance správce front stále spuštěna a odkaz na replikaci DR je stále funkční.
- Chcete-li změnit primární instanci správce front na sekundární instanci, zadejte tento příkaz:

  ```
  rdqmdr -m QMname -s
  ```
- Chcete-li zobrazit příkaz **crtmqm** požadovaný ke konfiguraci sekundární instance správce front, zadejte na svém primárním uzlu následující příkaz:

  ```
  rdqmdr -d -m QMname
  ```

  Můžete zadat vracený příkaz **crtmqm** na sekundárním uzlu, abyste mohli vytvořit sekundární instanci RD RDAM.

V 9.1.0 Linux *Spuštění, zastavení a zobrazení stavu DR RDQM*

Chcete-li spustit, zastavit a zobrazit aktuální stav replikovaného správce datových front zotavení z havárie (DR RDQM), použijete varianty standardních řídicích příkazů produktu IBM MQ .

Informace o této úloze

Musíte spustit příkazy, které spouštějí, zastavují a zobrazují aktuální stav replikovaného správce datových front (RDQM) jako uživatel, který patří do skupiny `mqm` .

Chcete-li spustit a zastavit správce front v primárním uzlu pro daného správce front (tj. v uzlu, v němž je správce front aktuálně spuštěn), musíte spustit příkazy.

Procedura

- Chcete-li spustit DR RDQM, zadejte na primárním uzlu RDQM tento příkaz:

  ```
  strmqm qmname
  ```

  kde *qmname* je název RDQM, který chcete spustit.
- Chcete-li zastavit RDQM, zadejte na primárním uzlu RDQM tento příkaz:

```
endmqm qmname
```

kde *qmname* je název RDQM, který chcete zastavit.

- Chcete-li zobrazit stav RDQM, zadejte tento příkaz:

```
dspmq -m QMname
```

Informace o stavu, které jsou výstupem, závisí na tom, zda jste spustili příkaz na primárním nebo sekundárním uzlu RDQM. Pokud se spustí na primárním uzlu, zobrazí se jedna z normálních stavových zpráv vrácených serverem **dspmq** . Spustíte-li příkaz na sekundárním uzlu, zobrazí se stav `Ended immediately` . Je-li například **dspmq** spuštěn na uzlu RDQM7, mohou být vráceny následující informace:

```
QMNAME(DRQM8)                           STATUS(Ended immediately)
QMNAME(DRQM7)                           STATUS(Running)
```

Můžete použít argumenty s `dspmq` k určení, zda je RDQM konfigurován pro zotavení z havárie, a zda je momentálně primární nebo sekundární instance:

```
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 správce front je konfigurován jako primární DR.

DRROLE(Secondary)
Označuje, že správce front je konfigurován jako sekundární server DR.

Související odkazy
dspmq
endmqm
strmqm

V 9.1.0 Linux

Zobrazení stavu DR RDQM

Můžete zobrazit stav všech replikovaných správců datových front (DR RQMs) replikace na uzlu nebo podrobné informace pro uvedené RDR.

Informace o této úloze

Příkaz **rdqmstatus** se používá k zobrazení stavu všech RDS DR nebo jednotlivých modulů RDQM.

Chcete-li spustit příkaz **rdqmstatus** , musíte být uživatel ve skupině `mqm` . Příkaz můžete spustit buď na jednom uzlu páru DR RDQM.

Procedura

- Chcete-li zobrazit stav všech RDQM DR na uzlu, spusťte na tomto uzlu následující příkaz:

```
rdqmstatus
```

Zobrazí se stav DR RDQMs na uzlu, například:

```
Queue manager name:                     DRQM8
Queue manager status:                   Ended immediately
DR role:                                Secondary

Queue manager name:                     DRQM7
Queue manager status:                   Running
DR role:                                Primary
```

- Chcete-li zobrazit stav konkrétního systému RDQM, zadejte tento příkaz:

```
rdqmstatus -m  qmname
```

Následující tabulka shrnuje informace, které jsou vráceny.

Tabulka 35. Atributy stavu

Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Stav správce front	stav (jak je zobrazeno v dspmq)	Vždy zobrazit
CPU	*n.nn*%	Pouze zobrazit, když má RDMQM v aktuálním uzlu primární roli
Paměť	*nnn*MB	Pouze zobrazit, když má RDMQM v aktuálním uzlu primární roli
Systém souborů správce front	*nnn*MB použito, *n.n*GB přiděleno [*n*%]	Pouze zobrazit, když má RDMQM v aktuálním uzlu primární roli
Role DR	Primární Sekundární Neznámý	Vždy zobrazit
Stav DR	Normální	Normální provoz
	Probíhá synchronizace	Probíhá synchronizace
	Rozděleno na oblasti	Správce front byl spuštěn na obou uzlech, zatímco síť replikace DR není k dispozici.
	Vzdálený systém je nedostupný	Připojení k jinému uzlu bylo ztraceno.
	Nekonzistentní	Synchronizace byla v průběhu zpracování, ale byla přerušena
	Návrat na snímek	Uživatel se rozhodl vrátit se k snímku, který byl proveden při vstupu správce front do nekonzistentním stavu.
	Vzdálený systém není konfigurován	Primární instance RDQM byla nakonfigurována, ale nebyla nakonfigurována žádná sekundární instance
	Nezdařená vyjednávání	Jeden z uzlů byl nastaven na synchronní replikaci a druhý na asynchronní replikaci
Typ DR	Synchronní nebo asynchronní	Vždy zobrazit
Port DR	*číslo_portu* (port TCP/IP použitý k replikaci dat pro tohoto správce front)	Vždy zobrazit
Lokální IP adresa DR	Lokální adresa IP, z níž je tento správce front kopírující z údajů pro DR	Vždy zobrazit

Tabulka 35. Atributy stavu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Vzdálená IP adresa DR	Vzdálená IP adresa, na kterou se tento správce front replikuje pro DR	Vždy zobrazit
Data DR nejsou synchronizována	*n*kB	Zobrazí se, když je vzdálený uzel nedostupný nebo nekonzistentní
Průběh synchronizace DR	*n*%	Zobrazí se, když probíhá synchronizace
Odhadovaný čas DR na dokončení	*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

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, když probíhá synchronizace:

```
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
```

Související odkazy

Linux rdqmstatus

V 9.1.0 Linux *Provoz v prostředí pro zotavení z havárie*

Existuje řada situací, ve kterých byste mohli chtít přepnout na sekundárního správce front v konfiguraci zotavení z havárie.

Zotavení z havárie

Po dokončení úplné ztráty primárního správce front na hlavním serveru spusťte sekundárního správce front na serveru pro zotavení. Aplikace se znovu připojí ke správci front na serveru obnovy a sekundární správce front zpracovává zprávy aplikace. Kroky provedené k vrácení zpět na předchozí konfiguraci závisí na příčině selhání. Například úplná ztráta hlavního uzlu versus dočasná ztráta.

Kroky k provedení dočasné ztráty hlavního serveru najdete v tématu “Přepnutí na uzel nápravy” na stránce 553. Chcete-li provést následující trvalé selhání, přečtěte si téma “Nahrazení selhaného uzlu v konfiguraci zotavení z havárie” na stránce 554.

Podpora testu zotavení z havárie

Konfiguraci zotavení z havárie můžete otestovat tak, že dočasně přepínáte na sekundární instanci a zkontrolujete, zda se aplikace mohou úspěšně připojit. Stejným postupem se řiďte stejným postupem, jako když přepnete po dočasném selhání primárního uzlu, viz “Přepnutí na uzel nápravy” na stránce 553.

Návrat na snímek

Pokud v primárním uzlu dojde k selhání během synchronizace, můžete se vrátit k snímku dat sekundárního správce front těsně před tím, než synchronizace začala. Sekundární se pak obnoví do konzistentního stavu a může být spuštěn jako primární. Chcete-li se vrátit ke snímku, proveďte sekundární funkci do primárního serveru, jak je popsáno v tématu “Přepnutí na uzel nápravy” na stránce 553. Před spuštěním správce front musíte zkontrolovat, zda bylo dokončeno vrácení zpět snímku (pomocí příkazu **rdqmstatus**).

V 9.1.0 Linux *Přepnutí na uzel nápravy*

Dojde-li k havárii v hlavním serveru, proveďte kroky k přepnutí na pracoviště obnovy.

Informace o této úloze

Po ztrátě primárního správce front na hlavní stránce můžete primární správce front na pracovišti obnovy převést na primární server a spustit jej. Aplikace se znovu připojí ke správci front na serveru obnovy a správce front zpracovává zprávy aplikací. Tuto proceduru můžete také použít k testování svého uzlu obnovy.

Důležité: Před povýšenou instancí sekundární instance je třeba zajistit, aby byla ukončena činnost primární instance správce front a aby byla provedena její sekundární instance. Jinak mohou být data rozdělena na oddíly.

Musíte být buď přihlášeni jako uživatel root, nebo jste přihlášeni jako uživatel, který patří do skupiny `mqm` , a má nezbytnou konfiguraci softwaru sudo.

Postup

1. Pokud tuto proceduru používáte 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. Zadáním následujícího příkazu na uzlu zotavení vytvořte sekundárního správce front v primárním uzlu:

```
rdqmdr -m qmname -p
```

3. Spusťte správce front zadáním následujícího příkazu:

```
strmqm qmname
```

4. Zkontrolujte, zda se vaše aplikace znovu připojí ke správci front ve správci front zotavení. Pokud jste definovali své kanály se seznamem alternativních názvů připojení, určujete-li primární a sekundární správce front, budou se aplikace automaticky připojovat k novému primárnímu správci front.

Související odkazy

strmqm

rdqmdr

Nahrazení selhaného uzlu v konfiguraci zotavení z havárie

Pokud ztratíte jeden z uzlů v konfiguraci zotavení z havárie, můžete nahradit uzel a obnovit konfiguraci zotavení z havárie následujícím postupem.

Informace o této úloze

Pokud dojde k havárii tak, že se uzel v hlavní lokalitě nachází mimo opravu, můžete nahradit selhaný uzel, zatímco je správce front spuštěn na uzlu obnovy a poté obnoví původní konfiguraci zotavení z havárie. Náhradní uzel musí převzít identitu uzlu, který selhal: název a adresa IP musí být stejné.

Musíte být buď přihlášeni jako uživatel root, nebo jste přihlášeni jako uživatel, který patří do skupiny `mqm` , a má nezbytnou konfiguraci softwaru sudo.

Postup

Po ztrátě správce front na hlavním serveru proveďte následující kroky:

1. Na 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 bude třeba 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. Zkontrolujte, zda se vaše aplikace znovu připojí ke správci front v uzlu zotavení. Pokud jste definovali své kanály se seznamem alternativních názvů připojení, určujete-li primární a sekundární správce front, budou se aplikace automaticky připojovat k novému primárnímu správci front.
5. Nahraďte uzel, který selhal, na hlavním serveru a nakonfigurujte jej tak, aby měl stejný název a adresu IP, kterou jste použili pro zotavení z havárie na původním uzlu. Poté proveďte konfiguraci zotavení z havárie spuštěním příkazu **crtmqm** , který jste zkopírovali v kroku 2. Nyní máte sekundární instanci správce front a primární instance synchronizuje svá data s sekundární instancí.
6. Ukončete aktuální primární instanci.
7. Po dokončení synchronizace zpřístupníte primární instanci, která je spuštěna na uzlu zotavení, do sekundárního serveru ještě jednou:

```
rdqmdr -m QMname -s
```

8. Na náhradním primárním uzlu proveďte sekundární instanci správce front v primární instanci:

```
rdqmdr -m QMname -p
```

9. Na náhradním primárním uzlu spusťte správce front:

```
strmqm QMname
```

   Nyní jste obnovili konfiguraci tak, jak byla před selháním na hlavním serveru.

Související odkazy
strmqm
rdqmdr
endmqm

Vyřešení nekonzistentního problému v DR RDQM
Stav DR `inconsistent` může být ohlášen, pokud dojde k selhání synchronizace mezi primární a sekundární instancí správce front.

Informace o této úloze

Nekonzistentní stav je hlášen na sekundární instanci správce front, protože během operace synchronizace došlo ke ztrátě připojení replikace k primární instanci. Je možné, že budete muset provést nějakou akci, abyste tuto situaci vyřešili. Zvažte následující posloupnost událostí:

1. Primární správce front DR v synchronizaci se sekundárním správcem front DR
2. Odkaz replikace byl ztracen mezi primárním a sekundárním serverem
3. Obnovený odkaz replikace mezi primárním a sekundárním serverem
4. Dojde k opětovné synchronizaci, kde sekundární správce front DR provede zachycení s primárním správcem front DR. Během této doby je stav DR serveru `synchronization in progress` vykazována pro oba správce front.
5. Je-li replikace během opětovné synchronizace znovu ztracena, bude stav na sekundárním serveru DR nahlášen jako `Inconsistent`.

Je-li uzel, který je hostitelem primárního správce front, stále funkční a lze obnovit replikační propojení, dojde k automatické opětovné synchronizaci. Nekonzistentní stav je vyřešen bez provedení jakékoli akce.

Pokud uzel, který je hostitelem primárního správce front, již není v provozu, můžete vyřešit nekonzistentní stav provedením vrácení snímku na snímek v sekundárním správci front. Tato operace vrátí data zpět do posledního známého dobrého stavu.

Postup

Chcete-li vyřešit nekonzistentní stav:

1. Na uzlu obnovení proveďte sekundární instanci do primární instance:

```
rdqmdr -m qmname -p
```

   Spustí se opětovné vrácení operace snímku.
2. Na uzlu nápravy zkontrolujte stav správce front, abyste viděli, kdy je operace vrácení zpět na snímek dokončena:

```
rdqmstatus -m qmname
```

3. Je-li stav správce front `Normal`, spusťte správce front:

```
strmqm qmname
```

Řešení problému rozděleného na oblasti (rozdělení mozku) v DR RDQM
Problém s dělením na oblasti se může vyskytnout, pokud se oba správci front v rámci dvojice zotavení z havárie v primární roli spouštějí současně.

Informace o této úloze

Pokud jste povýšili sekundární instanci správce front v uzlu pro zotavení, zatímco původní primární instance byla nadále spouštěna v hlavním uzlu, pak budete mít k dispozici dvě verze stejného správce front, přičemž každý z nich má vlastní pohled na data správce front. Stav DR pro správce front na každém uzlu se hlásí jako `Partitioned`.

Musíte se rozhodnout, který z těchto dvou správců front má nejsprávnější zobrazení dat, a zachovat tuto sadu při vyřazování z jiných. K provedení této operace se používá příkaz **rdqmdr** .

Procedura

- Chcete-li ponechat data od správce front v uzlu zotavení, postupujte takto:
  a) Ujistěte se, že obě instance správce front jsou zastaveny.
  b) Určete, zda je správce front v hlavním uzlu sekundárním serverem:

```
rdqmdr -m qmname -s
```

  c) Určete, že správce front v uzlu zotavení je primární:

```
rdqmdr -m qmname -p
```

  Zahájí se synchronizace s daty ze správce front na uzlu zotavení, který je kopírován do hlavního uzlu.
  d) Zkontrolujte stav synchronizace:

```
rdqmstatus -m qmname
```

  e) Po dokončení synchronizace snižte úroveň správce front v uzlu zotavení:

```
rdqmdr -m qmname -s
```

  f) Povýšit správce front v hlavním uzlu a spustit jej:

```
rdqmdr -m qmname -p
strmqm qmname
```

- Chcete-li ponechat data od správce front v hlavním uzlu:
  a) Ujistěte se, že obě instance správce front jsou zastaveny.
  b) Uveďte, zda je správce front v uzlu pro zotavení sekundární:

```
rdqmdr -m qmname -s
```

  c) Určete, že správce front v hlavním uzlu je primární uzel:

```
rdqmdr -m qmname -p
```

  Zahájí se synchronizace s daty ze správce front v hlavním uzlu, který je kopírován do uzlu nápravy.
  d) Zkontrolujte stav synchronizace:

```
rdqmstatus -m qmname
```

  e) Po dokončení synchronizace spusťte správce front v hlavním uzlu:

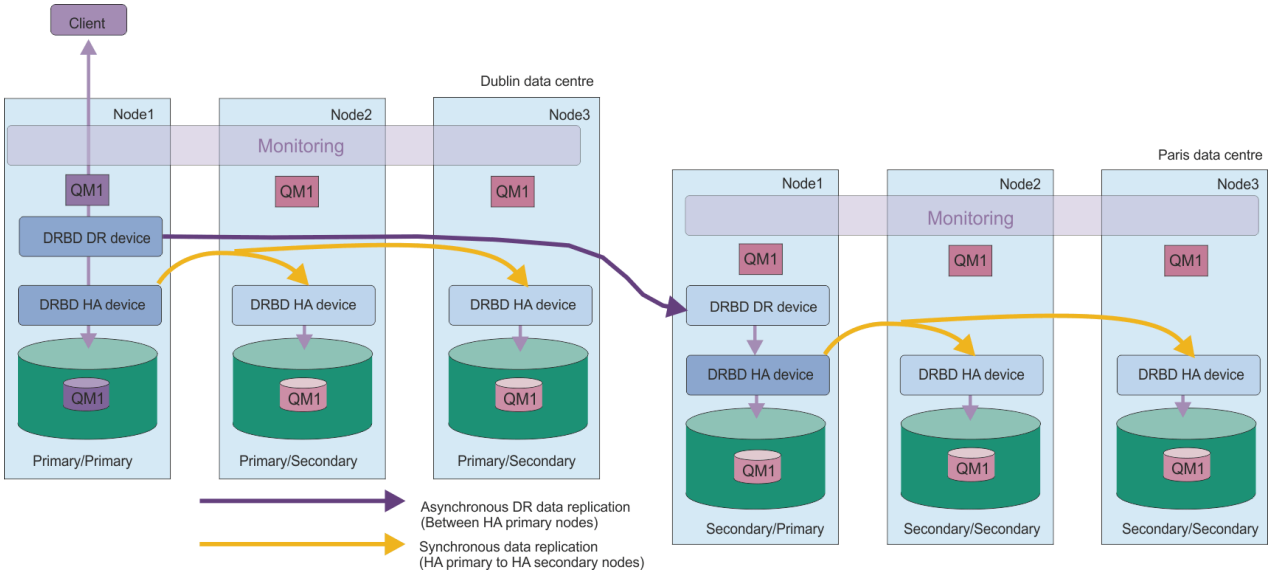
```
strmqm qmname
```

Linux V 9.1.5 Zotavení z havárie RDQM a zajištění vysoké dostupnosti

Můžete nakonfigurovat replikovaný správce datových front (RDQM), který se spustí ve skupině s vysokou dostupností na jednom serveru, ale může dojít k selhání na jinou skupinu s vysokou dostupností na jiném serveru, pokud dojde k nějaké katastrofě, která způsobí nedostupnost první skupiny. Toto je známo jako DR/HA RDQM.

DR/HA RDQM kombinuje funkce s vysokou dostupností RDQM (viz “Vysoká dostupnost RDQM” na stránce 513) a zotavení z havárie RDQM (viz “zotavení z havárie RDQM” na stránce 536).

Následující diagram znázorňuje příklad DR/HA RDQM.



Replikace mezi DR/HA RDQMs na hlavním serveru a serverem pro zotavení z havárie je vždy asynchronní. S asynchronní replikací jsou operace jako IBM MQ PUT nebo GET dokončeny a před replikací události do sekundárního správce front se vrátí do aplikace.

Je-li to nutné, můžete mít namísto 'main' a 'recovery' organizační jednotky místo 'main' a 'recovery', takže některé z vašich DR/HA RDQM běží na jednom serveru a některé na druhé v průběhu normálního provozu. Pokud dojde k havárii a dojde k znepřístupnění jednoho serveru, spustí se všechny RDQMs DR/HA ve stejné skupině HA na stejném serveru.

Každá skupina HA je konfigurována stejným způsobem jako běžná skupina HA. V každé skupině HA můžete definovat plovoucí adresy IP pro DR/HA RDQM. Plovoucí adresa IP může být stejná nebo odlišná pro každou skupinu HA.

Existující RDMS nemůžete povýšit na DR/HA RDQM, musíte vytvořit DR/HA RDQM. (Je-li to požadováno, můžete zálohovat data existujícího RDQM, odstranit jej, znovu vytvořit jako DR/HA RDQM, a pak obnovit data, viz “Zálohování a obnova dat správce front produktu IBM MQ” na stránce 601.)

Chcete-li konfigurovat DR/HA RDQMs, musíte dokončit 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 'main'.
4. Na ostatních dvou uzlech v hlavní lokalitě vytvořte primární/sekundární DR/HA DRQMs.
5. Definujte plovoucí adresu IP pro aplikaci k přístupu do DR/HA RDQM, je-li spuštěna na libovolném uzlu skupiny HA na hlavním serveru 'main'.
6. Vytvořte sekundární/primární DR/HA RDQM na jednom uzlu skupiny s vysokou dostupností na serveru 'recovery'.
7. Vytvořte sekundární/sekundární DR/HA RDQMs na dalších dvou uzlech v organizační jednotce 'recovery'.

8. Definujte plovoucí adresu IP pro aplikaci k přístupu do DR/HA RDQM, je-li spuštěna na libovolném z uzlů skupiny HA na serveru 'recovery'.

Podrobnosti o každém z těchto kroků jsou uvedeny v následujících tématech.

Linux V 9.1.5 *Požadavky na řešení DR/HA RDQM*

Požadavky na řešení RD/HA RDQM jsou stejné jako pro řešení RDQM HA a řešení DR RDQM.

Podrobné informace o požadavcích na součásti HA konfigurace viz “Požadavky pro řešení RDQM HA” na stránce 515.

Podrobnosti o části DR pro konfiguraci viz “Požadavky pro řešení DR RDQM” na stránce 539.

Linux V 9.1.5 *Konfigurace skupin HA pro DRQMs DR/HA*

Je třeba vytvořit skupinu HA na hlavním pracovišti i na serverech pro zotavení. Máte-li na organizační jednotce existující skupinu s vysokou dostupností, můžete ve skupině HA vytvořit DR/HA RDQMs. (Existující RDQM budou i nadále fungovat jako dříve.)

Procedura je stejná, jak je popsáno pro vysokou dostupnost RDQM, viz “Definování klastru Pacemaker (HA group)” na stránce 518.

Při definování skupiny s vysokou dostupností určíte adresy IP, které se používají pro monitorování a replikaci každým uzlem v souboru `rdqm.ini` . Při vytváření skupiny HA pro podporu DR/HA RDQMs můžete také uvést adresy IP použité pro replikaci DR skupinou HA, kterou definujete, a adresy IP použité pro replikaci DR uzly ve druhé skupině HA páru DR. (Pokud v souboru `rdqm.ini` neuvedete adresy IP replikace DR, můžete je zadat na příkazovém řádku, když vytvoříte DR/HA RDQM.)

Pokud konfigurujete existující skupinu HA, můžete do existujícího souboru `rdqm.ini` přidat adresy IP replikace DR. Nemusíte znovu spouštět **rdqmadm** po aktualizaci `rdqm.ini`, ale musíte aktualizovat `rdqm.ini` před tím, než vytvoříte DR/HA RDQMs.

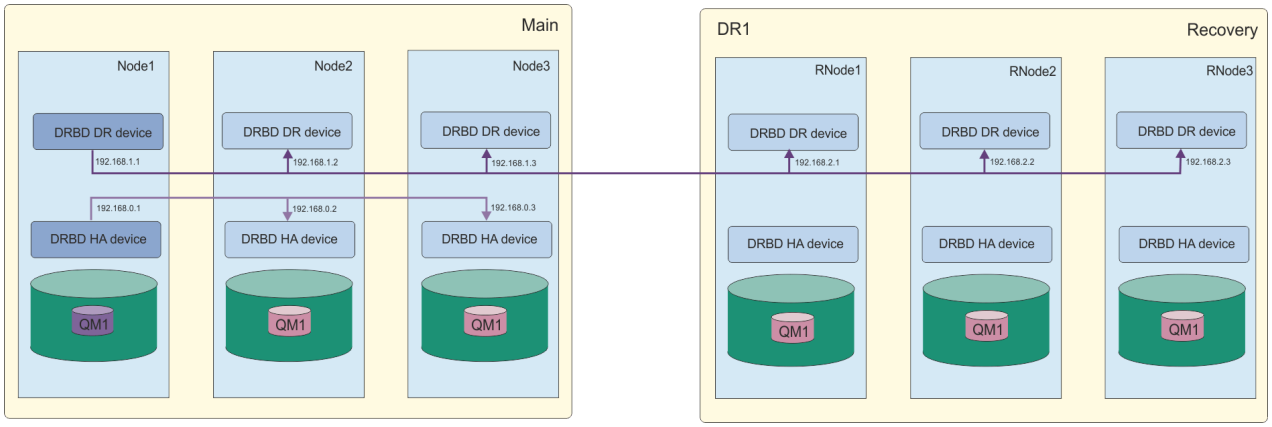
Použijte atribut `DR_Replication` ve stanzách `Node` , abyste uvedli rozhraní replikace DR na skupině HA, kterou definujete, například:

```
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
```

Použijte stanzu `DRGroup` 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
```

Tato konfigurace ilustruje následující diagram:



Pokud neurčíte adresy IP replikace DR pro uzly v lokální skupině s vysokou dostupností v souboru `rdqm.ini` nebo na příkazovém řádku při vytváření DR/HA RDQM, pak jsou rozhraní `HA_Replication` definovaná pro každý uzel použita pro replikaci DR. Musíte zadat adresy vzdálené replikace DR skupiny DR buď v souboru `rdqm.ini` , nebo na příkazovém řádku **`crtmqm`** .

Linux V 9.1.5 *Vytváření dat DR/HA RDQMs*

K vytvoření replikovaného správce datových front (RDQM) v konfiguraci DR/HA se používá příkaz **`crtmqm`** .

Informace o této úloze

Pokud uživatel může použít příkaz sudo, můžete vytvořit DR/HA RDQM jako uživatele ve skupině `mqm` . Jinak musíte vytvořit RDQM jako kořen.

Musíte vytvořit číslo DR/HA RDQMs:

- Ve skupině HA na hlavní stránce:
  - V uzlu, v němž má být správce front spuštěn za normálních podmínek, vytvořte primární/primární DR/HA RDQM.
  - Na každém z ostatních dvou uzlů ve skupině HA vytvořte primární/sekundární DR/HA RDQM.
- Ve skupině HA na serveru 'Recovery':
  - Na uzlu, v němž bude spuštěn správce front, pokud dojde k selhání na serveru pro zotavení, vytvořte sekundární/primární DR/HA RDQM. Výstup příkazu můžete použít, když jste vytvořili primárního/primárního správce front na hlavní stránce 'main'.
  - Na každém z ostatních dvou uzlů ve skupině HA vytvořte sekundární/sekundární DR/HA RDQM.

Všechny instance správce front musí mít stejný název a musí být přiděleny stejné množství úložiště.

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 určete adresy IP rozhraní DR na třech uzlech na lokálním serveru (tj. na hlavní stránce 'hlavního'). Není-li tento parametr zadán, použijí se adresy IP zadané v souboru `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Zadejte adresy IP rozhraní DR na třech uzlech na vzdáleném serveru (tj. na pracovišti 'recovery'). Musíte zadat buď tento parametr, nebo argument `-rn` .

-rn *GroupName*
Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

-rp *Port*
Uvádí port, který se má použít pro replikaci DR.

other_crtm_qm_options
Volitelně můžete zadat jednu nebo více z těchto obecných voleb obslužného programu **`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 svazku, který je vytvořen ve skupině svazků drbdpool. Je také vytvořen jiný logický svazek této velikosti, který podporuje návrat k operaci snímku, takže celkové úložiště pro DR RDQM je právě více než dvojnásobek, které je zde uvedeno.

QMNAME
Určuje název replikovaného správce datových front. V názvu jsou rozlišována velká a malá písmena.

Po dokončení příkazu vypíše příkaz, který můžete zadat na serveru pro zotavení, a vytvořit tak sekundární/primární instanci správce front.

- Chcete-li vytvořit primární/sekundární RDQM DR/HA na ostatních dvou uzlech ve skupině HA, postupujte takto:

  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:

-sx
Označuje, že počáteční role HA je sekundární.

-rr p
Označuje, že počáteční role DR je primární.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Volitelně určete adresy IP rozhraní DR na třech uzlech na lokálním serveru (tj. na hlavní stránce 'hlavního'). Není-li tento parametr zadán, použijí se adresy IP zadané v souboru `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Zadejte adresy IP rozhraní DR na třech uzlech na vzdáleném serveru (tj. na pracovišti 'recovery'). Musíte zadat buď tento parametr, nebo argument `-rn` .

-rn *GroupName*
Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

-rp *Port*
Uvádí port, který se má použít pro replikaci DR.

-fs *velikost*
Uvádí velikost systému souborů, který se má vytvořit pro správce front, tj. velikost logického svazku, který je vytvořen ve skupině svazků drbdpool. Pokud jste při vytváření primárního/primárního RDQM zadali jinou než výchozí velikost, musíte zde zadat stejnou hodnotu.

QMNAME
Uvádí název primárního/sekundárního RDQM. Musí to být stejné jako jméno, které jste uvedli pro primární/primární instanci RDQM. Všimněte si, že název rozlišuje velikost písmen.

- Chcete-li vytvořit sekundární/primární RDR/QM RDQM na uzlu, kde se správce front spustí, pokud dojde k selhání na serveru pro 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 můžete zadat adresy IP rozhraní DR na třech uzlech na lokálním serveru (tj. na stránce 'obnova'). Není-li tento parametr zadán, použijí se adresy IP zadané v souboru `rdqm.ini` .

-ri *DRRemoteIP1*, *DRRemoteIP2*, *DRRemoteIP3*
Zadejte adresy IP rozhraní DR na třech uzlech na vzdáleném serveru (tj. na hlavní stránce 'hlavního'). Musíte zadat buď tento parametr, nebo argument `-rn` .

-rn *GroupName*
Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

-rp *Port*
Uvádí port, který se má použít pro replikaci DR.

-fs *velikost*
Volitelně určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického svazku, který je vytvořen ve skupině svazků drbdpool. Je také vytvořen jiný logický svazek této velikosti, který podporuje návrat k operaci snímku, takže celkové úložiště pro DR RDQM je právě více než dvojnásobek, které je zde uvedeno.

QMNAME
Určuje název replikovaného správce datových front. V názvu jsou rozlišována velká a malá písmena.

- Vytvoření sekundárního/sekundárního HA/DR RDQM na ostatních dvou uzlech na serveru pro obnovu:
  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
```

-sx
Označuje, že počáteční role HA je primární.

-rr s
Označuje, že počáteční role DR je sekundární.

-rl *DRLocalIP1*, *DRLocalIP2*, *DRLocalIP3*
Volitelně můžete určit adresy IP rozhraní DR na třech uzlech na lokálním serveru. Není-li tento parametr zadán, použijí se adresy IP zadané 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 argument `-rn` .

-rn *GroupName*
Uveďte název vzdálené skupiny HA, jak je uvedeno v souboru `rdqm.ini` . Musíte zadat buď `-ri` , nebo `-rn`.

-rp *Port*
Uvádí port, který se má použít pro replikaci DR.

-fs *velikost*
Volitelně určuje velikost systému souborů, který má být vytvořen pro správce front, tj. velikost logického svazku, který je vytvořen ve skupině svazků drbdpool. Je také vytvořen jiný logický svazek této velikosti, který podporuje návrat k operaci snímku, takže celkové úložiště pro DR RDQM je právě více než dvojnásobek, které je zde uvedeno.

QMNAME
Určuje název replikovaného správce datových front. V názvu jsou rozlišována velká a malá písmena.

Jak pokračovat dále

Po vytvoření všech DR/HA RDQMs je třeba zkontrolovat stav primárních/primárních a sekundárních/primárních instancí, abyste zkontrolovali vše, co je 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 564. Pokud tento stav nezobrazujete, odstraňte sekundární/primární instanci a znovu ji vytvořte, přičemž je třeba dbát na správné argumenty.

Související úlohy

“Vytváření dat DR/HA RDQMs” na stránce 559
K vytvoření replikovaného správce datových front (RDQM) v konfiguraci DR/HA se používá příkaz **crtmqm** .

Související odkazy

crtmqm

Linux V 9.1.5 *Odstranění DR/HA RDQM*

K odstranění replikovaného datového správce front DR/HA (RDQM) se používá příkaz **dltmqm** .

Informace o této úloze

Musíte spustit příkaz k odstranění RDMQM na primárním/primárním uzlu i na sekundárním/primárním uzlu. RDQM musí být ukončen první. Příkaz můžete spustit jako uživatel mqm, pokud má tento uživatel potřebná oprávnění k příkazu sudo. Jinak musíte spustit příkaz jako uživatel root.

Procedura

- Chcete-li odstranit DR/HA RDQM, zadejte následující příkaz:

```
dltmqm RDQM_name
```

Související odkazy

dltmqm

Linux V 9.1.5 ***Vytvoření plovoucí adresy IP***

Můžete vytvořit plovoucí adresy IP pro každou ze skupin HA v konfiguraci dat DR/HA RDQM.

Plovoucí adresa IP umožňuje klientovi použít stejnou adresu IP pro DR/HA RDQM bez ohledu na uzel ve skupině HA, na které je spuštěný. Mají-li vaše dvě skupiny vysoké dostupnosti soukromé/izolované sítě pro konektivitu aplikace, pak lze pro obě skupiny definovat stejnou plovoucí adresu IP. Musíte však stále definovat tuto plovoucí adresu IP dvakrát, avšak jednou pro každou ze skupin HA.

Plovoucí adresy IP můžete vytvářet a odstraňovat pomocí stejné metody jako u RDQM HA. Viz “Vytvoření a odstranění plovoucí adresy IP” na stránce 529.

Linux V 9.1.5 ***Spuštění, zastavení a zobrazení stavu DR/HA RDQM***

Chcete-li spustit, zastavit a zobrazit aktuální stav DR/HA RDQM, použijte varianty standardních řídicích příkazů IBM MQ .

Informace o této úloze

Musíte spustit příkazy, které začínají, zastavují a zobrazují aktuální stav DR/HA RDQM jako uživatel, který patří do skupin `mqm` a `haclient` .

Chcete-li spustit a zastavit správce front v primárním uzlu pro daného správce front, je třeba spustit příkazy.

Procedura

- Chcete-li spustit RDQM, zadejte na primárním uzlu RDQM tento příkaz:

```
strmqm qmname
```

  kde *název_qmname* je název DR/HA RDR, který chcete spustit.

  RDQM je spuštěn a Pacemaker spustí správu RDQM. Chcete-li zadat jakékoli jiné volby `strmqm` , musíte zadat volbu `-ns` s volbou `strmqm` .
- Chcete-li zastavit RDQM, zadejte na primárním uzlu DR/HA RDQM tento příkaz:

```
endmqm qmname
```

  kde *qmname* je název RDQM, který chcete zastavit.

  Pacemaker přestane spravovat RDQM, a pak se ukončí RDQM. Všechny ostatní parametry **endmqm** mohou být použity při zastavení RDQM.
- Chcete-li zobrazit stav RDQM, zadejte tento příkaz:

```
dspmq -m QMname
```

Informace o stavu, které jsou výstupem, závisí na tom, zda jste spustili příkaz na primárním nebo sekundárním uzlu RDQM. Pokud se spustí na primárním uzlu, zobrazí se jedna z normálních stavových zpráv vrácených serverem **dspmq** . Spustíte-li příkaz na sekundárním uzlu, zobrazí se stav Ended immediately . Je-li například **dspmq** spuštěn na uzlu RDQM7, mohou být vráceny následující informace:

```
QMNAME(DRQM8)                           STATUS(Ended immediately)
QMNAME(DRQM7)                           STATUS(Running)
```

Můžete použít argumenty s dspmq k určení, zda je RDQM konfigurován pro zotavení z havárie, a zda je momentálně primární nebo sekundární instance:

```
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 správce front je konfigurován jako primární DR.

DRROLE(Secondary)
Označuje, že správce front je konfigurován jako sekundární server DR.

Použijte příkaz **dspmq -o all** k zobrazení informací o zotavení z havárie a vysoké dostupnosti pro DR/HA RDQMs. Pokud například spustíte příkaz **dspmq -o all** na uzlu, na kterém je spuštěný DR/HA RDQM, zobrazí se následující informace o stavu:

```
QMNAME(TESTQM1)                                           STATUS(Running) HA(Replicated)
DRROLE(Primary)
```

Související odkazy
dspmq (zobrazení správců front)
endmqm (ukončit správce front)
strmqm (spuštění správce front)

Linux V 9.1.5 ***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.

Chcete-li spustit příkaz **rdqmstatus** , musíte být uživatelem ve skupinách mqm a hacliient . Příkaz můžete spustit na libovolném uzlu v jedné ze skupin HA.

Procedura

- Chcete-li zobrazit 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

Queue manager name:                     RDQM1
```

```
Queue manager status:                  Running elsewhere
HA current location:                   main-charlie

Queue manager name:                    RDQM9
Queue manager status:                  Running elsewhere
HA current location:                   main-bob
DR role:                               Primary

Queue manager name:                    RDQM7
Queue manager status:                  Running
HA current location:                   This node
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.

- 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.

Následující tabulka shrnuje informace o aktuálním uzlu, které mohou být vráceny příkazem **rdqmstatus** pro RDQM.

Tabulka 36. 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
Role HA	Primární Sekundární V 9.1.5 Sekundární nevyřízený 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

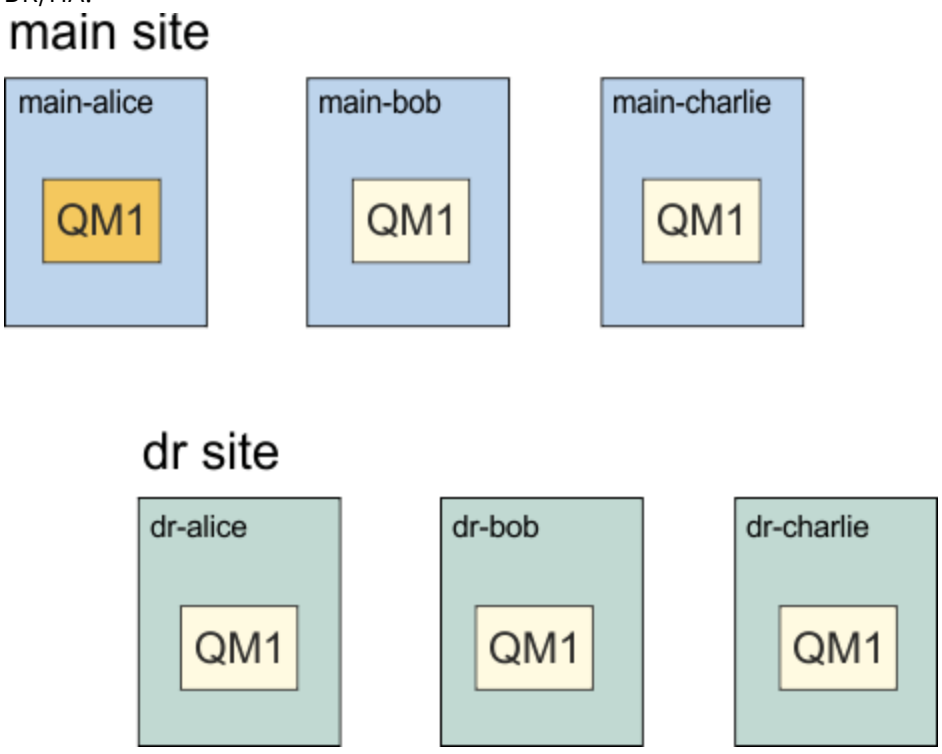
Tabulka 36. Aktuální stav uzlu (pokračování)

Atribut Stav	**Možné hodnoty**	**Při zobrazení**
Upřednostňované umístění HA	Není Tento uzel Neznámý *NodeName*	Vždy zobrazeno
Plovoucí rozhraní IP HA	*název_rozhraní*	Vždy zobrazeno
Plovoucí adresa IP HA	*IPV4_address*	Vždy zobrazeno
Role DR	Primární Sekundární Neznámý	Vždy zobrazeno
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, když 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.

Tabulka 36. Aktuální stav uzlu (pokračování)		
Atribut Stav	**Možné hodnoty**	**Při zobrazení**
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.
Průběh opětovného vrácení snímku	*y*%	Zobrazí se, když je stav DR "Návrat ke snímku"

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 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 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 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 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 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 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
```

Související odkazy

Linux rdqmstatus

V 9.1.0 Linux ***Obsluha v prostředí DR/HA***

Při práci v prostředí DR/HA jsou k dispozici samostatné pokyny pro zajištění vysoké dostupnosti a zotavení z havárie.

Pokud selže uzel, na kterém je spuštěn DR/HA RDQM, RDQM automaticky překoná selhání na jiný uzel ve skupině HA. Pokud dojde k selhání celého serveru, musíte ručně spustit RDQM na upřednostňovaném uzlu ve skupině HA na serveru pro zotavení. Zde uvedené aspekty jsou stejné jako u běžného RDQM, viz “Provoz v prostředí pro zotavení z havárie” na stránce 553 , kde získáte další informace.

Pokud dojde k úplnému selhání jednoho z uzlů a je třeba jej nahradit, viz “Nahrazení selhaného uzlu v konfiguraci zotavení z havárie” na stránce 554 a “Náhrada vadného uzlu v konfiguraci vysoké dostupnosti” na stránce 535 , kde jsou uvedeny pokyny.

Linux V 9.1.5 ***Nahrazení uzlu, který selhal, v konfiguraci DR/HA***

Pokud jeden z uzlů ve vašich skupinách vysoké dostupnosti selže, můžete jej nahradit.

Informace o této úloze

Postup se liší v závislosti na tom, zda je uzel, který nahrazujete, primární nebo sekundární v konfiguraci DR. V obou případech musí mít nový uzel stejnou konfiguraci na uzel, který nahrazujete, tj. musí mít stejný název hostitele, stejné adresy IP a podobně.

Můžete se také setkat se situací, kdy jste zcela ztratili skupinu HA na hlavním pracovišti nebo na pracovišti obnovy a že jste museli nahradit celou skupinu HA.

Procedura

- U náhradního uzlu, který je primární v konfiguraci DR, proveďte na novém uzlu následující kroky:
  a) Vytvořte soubor `rdqm.ini` , který se shoduje se soubory na jiných uzlech, a poté spusťte příkaz `rdqmadm -c` (viz “Definování klastru Pacemaker (HA group)” na stránce 518).
  b) Spusťte příkaz `crtmqm -sxs -rr p` *qmanager* a znovu vytvořte všechny DR/HA RDQM (viz “Vytváření dat DR/HA RDQMs” na stránce 559).
- U náhradního uzlu, který je sekundární v konfiguraci DR, proveďte na novém uzlu následující kroky:
  a) Vytvořte soubor `rdqm.ini` , který se shoduje se soubory na jiných uzlech, a poté spusťte příkaz `rdqmadm -c` (viz “Definování klastru Pacemaker (HA group)” na stránce 518).
  b) Spusťte příkaz `crtmqm -sx -rr s` *qmanager* k novému vytvoření každého DR/HA RDQM (viz “Vytváření dat DR/HA RDQMs” na stránce 559).
- Chcete-li nahradit celou skupinu HA, proveďte následující kroky:
  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 mohli pokračovat ve spouštění vašich DR/HA RDQMs (viz “Provoz v prostředí pro zotavení z havárie” na stránce 553). (Pokud ztratíte celou skupinu HA na pracovišti obnovy, vaše RDQM DR/HA jsou nadále spuštěny na hlavní stránce bez vašeho zásahu.)
  b) Znovu vytvořte skupinu HA na třech náhradních uzlech, jak je popsáno v tématu “Konfigurace skupin HA pro DRQMs DR/HA” na stránce 558.
  c) Znovu vytvořte RDQMs DR/HA na nové skupině HA, jak je popsáno v tématu “Vytváření dat DR/HA RDQMs” na stránce 559.
  d) Je-li to nutné, proveďte spravované překonání selhání ze serveru pro zotavení zpět na hlavní server.

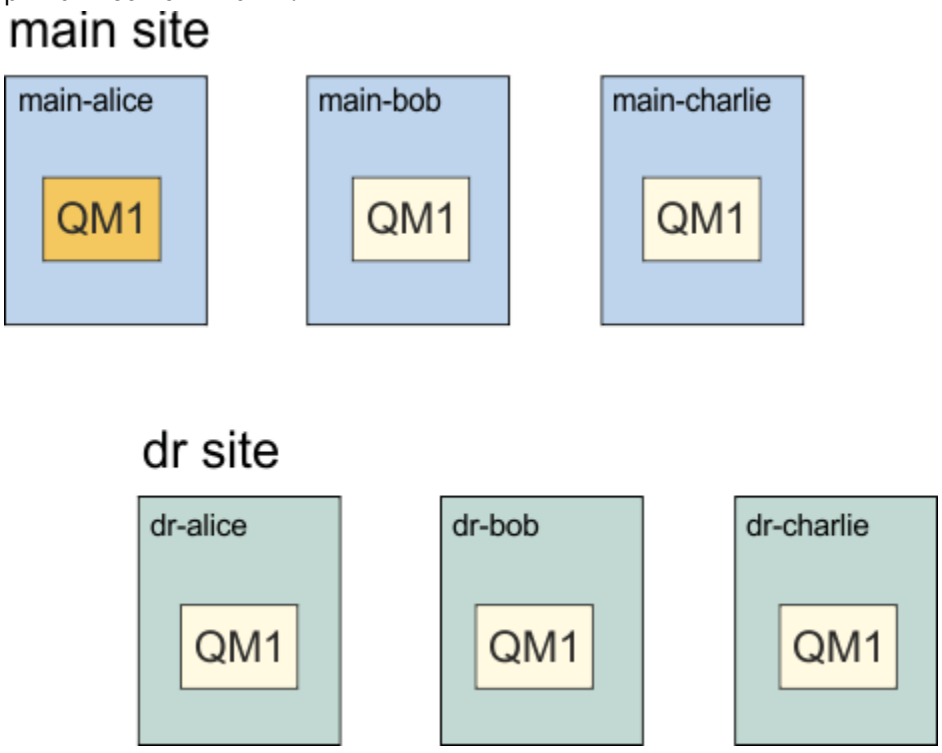
Linux V 9.1.5 ***Příklad odpracované DR/HA RDQM***

Tento příklad ukazuje, jak vytvořit a odstranit DR/HA RDQM.

Vytvoření DR/HA RDQM

Příklad konfigurace má dvě organizační jednotky nazvané 'main' a 'dr'. Každý server má tři uzly s názvem 'alice', 'bob' a 'charlie'. Uzly mají úplný název skládající se z jejich názvu serveru a názvu, takže 'main-alice', 'dr-alice' a tak dále.

Následující kroky vytvoří DR/HA RDQM s názvem QM1 , které běží na main-alice. Hlavní uzel alice je primární server HA a DR.



Pokud jsou v souboru `rdqm.ini` zadány lokální a vzdálené IP adresy DR, pak není třeba uvádět adresy IP na příkazovém řádku a DR/HA RDQM s názvem QM1 lze vytvořit spuštěním následujícího příkazu na hlavním ledě:

```
crtmqm -sx -rr p -rn DR1 -rp 7001 QM1
```

Jsou-li v souboru `rdqm.ini` zadány lokální adresy IP DR, lze na příkazovém řádku zadat adresy IP vzdáleného systému DR:

```
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` určeny žádné adresy IP DR, lze na příkazovém řádku zadat jak vzdálenou, tak lokální adresu IP DR:

```
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 v odezvě 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, chcete-li vytvořit 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 instanci DR

Chcete-li otestovat funkce zotavení z havárie pro QM1, spusťte následující příkaz na hlavní alici, abyste učinili QM1 sekundární instanci 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 instanci 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, ukončete nejprve správce front v hlavním systému alice:

```
endmqm -w QM1
Replicated data queue manager disabled.
Waiting for queue manager 'QM1' to end.
IBM MQ queue manager 'QM1' ended.
```

Poté spusťte následující příkaz na hlavním ledě a odstraňte 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

“Obsluha v prostředí DR/HA” na stránce 569
Při práci v prostředí DR/HA jsou k dispozici samostatné pokyny pro zajištění vysoké dostupnosti a zotavení z havárie.

Související úlohy

“Vytváření dat DR/HA RDQMs” na stránce 559
K vytvoření replikovaného správce datových front (RDQM) v konfiguraci DR/HA se používá příkaz **crtmqm** .

“Odstranění DR/HA RDQM” na stránce 563
K odstranění replikovaného datového správce front DR/HA (RDQM) se používá příkaz **dltmqm** .

Protokolování: Ujištění se, že zprávy nejsou ztraceny

Příkaz IBM MQ zaznamenává všechny významné změny trvalých dat řízených správcem front v protokolu pro zotavení.

To zahrnuje vytváření a odstraňování objektů, trvalé aktualizace zpráv, stavy transakcí, změny atributů objektů a aktivity kanálu. Protokol obsahuje informace, které potřebujete k obnově všech aktualizací do front zpráv pomocí:

- Uchovávání záznamů o změnách správce front
- Uchovávání záznamů aktualizací fronty pro použití procesem restartování
- Povolení obnovy dat po selhání hardwaru nebo softwaru

Produkt IBM MQ se však také spoléhá na diskový systém, který je hostitelem jeho souborů, včetně souborů protokolu. Je-li diskový systém sám o sobě nespolehlivý, mohou být informace, včetně informací o protokolu, ztraceny.

POZOR: Protokoly pro zotavení nelze přesouvat do jiného operačního systému.

Jaké protokoly vypadají jako

Protokoly se skládají z primárních a sekundárních souborů a řídicího souboru. Definujete počet a velikost souborů protokolu a umístění, kde jsou uloženy v systému souborů.

Protokol IBM MQ se skládá ze dvou komponent:

1. Jeden nebo více souborů dat protokolu.
2. Řídicí soubor protokolu

Soubor dat protokolu je také znám jako oblast protokolu.

Existuje mnoho oblastí protokolu, které obsahují zaznamenaná data. Můžete definovat počet a velikost (jak je vysvětleno v části “Sekce LogDefaults souboru mqs.ini” na stránce 91), nebo provést výchozí nastavení systému tří primárních a dvou sekundárních fyzických oblastí.

Každá ze tří primárních a dvou sekundárních oblastí pro rozšíření je standardně 16 MB.

Při vytvoření správce front je počet předem přidělených rozsahů protokolu k počtu přidělených oblastí *primární* oblasti protokolu. Pokud číslo nezadáte, 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 574.

Windows Pokud jste v produktu IBM MQ for Windowsnezměnili cestu k protokolu, dojde k vytvoření oblastí protokolu v adresáři:

```
C:\ProgramData\IBM\MQ\log\QMgrName
```

ULW Pokud jste v produktu IBM MQ for UNIX and Linux nezměnili cestu k protokolu, vytvoří se oblasti pro rozšíření protokolu pod adresářem:

```
/var/mqm/log/QMgrName
```

IBM MQ začíná s těmito oblastmi primárního protokolu, ale pokud není primární prostor žurnálu dostatečný, alokuje *sekundární* oblasti protokolu pro rozšíření. To dělá dynamicky a odstraňuje je, když se sníží poptávka po protokolovaných prostorech. Standardně může být alokováno až dva rozšíření sekundárních protokolů. Tuto výchozí alokaci můžete změnit, jak je popsáno v tématu "Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms" na stránce 81.

Rozsahy protokolu mají předponu buď o písmeno S , nebo o písmeno R. Aktivní, neaktivní a nadbytečné fyzické oblasti mají předponu S, zatímco opětovné použití oblastí pro rozšíření je předponou R.

Při zálohování nebo obnově vašeho správce front proveďte zálohu a obnovu všech aktivních, neaktivních a nadbytečných oblastí spolu s řídicím souborem protokolu.

Poznámka: Nemusíte zálohovat a obnovovat opětovné použití oblastí pro rozšíření.

Soubor řízení žurnálu

Řídicí soubor protokolu obsahuje informace potřebné k popisu stavu fyzických oblastí protokolu, jako je jejich velikost a umístění, a název další dostupné oblasti.

Důležité: Řídicí soubor protokolu je určen pouze pro interní použití správce front.

Správce front uchovává řídicí data přidružená ke stavu protokolu pro zotavení v řídicím souboru protokolu a vy nesmíte upravit obsah řídicího souboru protokolu.

Řídicí soubor protokolu se nachází v cestě k protokolu a nazývá se `amqhlctl.lfh`. Při zálohování nebo obnově vašeho správce front se ujistěte, že je soubor řízení protokolu zálohován a obnoven spolu s oblastmi protokolu.

Typy protokolování

V produktu IBM MQ existují dva způsoby udržování záznamů o aktivitách správce front: kruhové protokolování a lineární protokolování.

Kruhové protokolování

Použijte kruhové protokolování, pokud chcete, aby obnova restartoval, použijte protokol k odvolání transakcí, které probíhaly, když se systém zastavil.

Kruhové protokolování zachová všechna data restartování v kruhu souborů protokolu. Protokolování vyplní první soubor v kruhu a poté vždy přejde na další, dokud nejsou naplněny všechny soubory. Nakonec přejde na první soubor v kruhu a začne znovu. Tento postup probíhá po celou dobu používání protokolu a má výhodu, že nikdy nedojde k nedostatku souborů protokolu.

Produkt IBM MQ uchovává záznamy protokolu vyžadované k restartování správce front bez ztráty dat, dokud tyto záznamy nebudou nadále vyžadovány k zajištění zotavení dat správce front. Mechanismus pro uvolnění souborů protokolu pro opětovné použití je popsán v tématu "Použití kontrolního bodu k zajištění úplné obnovy" na stránce 576.

lineární protokolování

Použijte lineární protokolování, chcete-li jak obnovu znovuspuštění, tak obnovu médií (opětovné vytvoření ztracených nebo poškozených dat opětovným přehráváním obsahu protokolu). Lineární protokolování uchovává protokolovaná data v souvislé posloupnosti souborů protokolu.

Soubory protokolu mohou být volitelně:

- Opětovné použití, ale pouze v případě, že již nejsou potřebné k restartování obnovy nebo zotavení média.
- Ručně archivováno pro dlouhodobé uložení a analýzu.

Frekvence obrazů médií určuje, kdy lze znovu použít lineární soubory protokolu, a je hlavním faktorem toho, kolik místa na disku musí být k dispozici pro lineární soubory protokolů.

Správce front můžete nakonfigurovat tak, aby automaticky přijal pravidelné obrazy médií, a to buď na základě času, nebo využití protokolu, nebo můžete obrazy médií naplánovat ručně.

Váš administrátor rozhodne, jaká zásada se má implementovat, a důsledky na využití prostoru na disku. Soubory žurnálu potřebné pro restart musí být vždy dostupné, zatímco soubory protokolů potřebné pouze pro obnovu médií lze archivovat do delšího termínu úložiště, například z pásky.

Pokud administrátor povolí automatickou správu protokolů a automatické obrazy média, bude se lineární protokolování chovat podobně jako velmi velký kruhový protokol, ale s vyšší redundancí proti selhání média umožněným obnovou médií.

V 9.1.0 V produktu IBM MQ 9.1.0 můžete změnit existující typ protokolu pro správce front z lineárního na kruhové nebo z kruhové na lineární pomocí příkazu migmqlog .

Fyzické oblasti protokolu v lineárním protokolu, které nejsou aktivní

V 9.1.0 Multi

Pokud v produktu IBM MQ 9.1.0používáte automatické správy protokolů včetně archivace, modul protokolování sleduje oblasti s lineárním protokolem protokolu, které nejsou aktivní.

Upozornění: Pokud používáte automatické správy protokolů, bez archivace, použití správce front zálohování není pro tento proces podporováno.

ULW Pokud již není oblast protokolu pro zotavení již vyžadována a v případě potřeby je archivována, bude modul protokolování na vhodném místě buď odstranit oblast protokolu, nebo ji znovu použít.

Opětovně použitá oblast protokolu je přejmenována na další v posloupnosti protokolu. Zpráva AMQ7490 je pravidelně zapisována s uvedením počtu oblastí, které byly vytvořeny, odstraněny nebo znovu použity.

Modul protokolování vybere, kolik oblastí má být připraveno k opětovnému použití a kdy má být tyto fyzické oblasti odstraněny.

Aktivní protokol

Existuje celá řada souborů, které se říká, že jsou *aktivní* v obou lineárních a kruhových protokolování. Aktivní protokol je maximální množství protokolovacího prostoru, ať už používáte kruhové nebo lineární protokolování, které může být odkazováno restartováním nápravy.

Počet aktivních souborů protokolu je obvykle menší než počet primárních souborů protokolu, jak je definováno v konfiguračních souborech. (Informace o definování čísla naleznete v tématu “Výpočet velikosti protokolu” na stránce 579 .)

Všimněte si, že aktivní protokolovací prostor nezahrnuje prostor potřebný pro obnovu médií a že počet souborů protokolu použitých s lineárním protokolováním může být velmi velký, v závislosti na toku zpráv a frekvenci obrazů médií.

Neaktivní protokol

Není-li již soubor protokolu potřebný pro obnovení restartování, stane se *neaktivní*. Soubory protokolu, které nejsou povinné pro obnovu po restartu, nebo obnovu médií, lze považovat za nadbytečné soubory protokolu.

Při použití automatického správy protokolů správce front řídí zpracování těchto zbytečných souborů protokolu. Pokud jste zvolili ruční správu protokolů, stává se odpovědností administrátora spravovat (například odstraňovat a archivovat) nadbytečné soubory žurnálu, pokud již nejsou pro vaši operaci zajímavé.

Další informace o odebírání souborů protokolu naleznete v příručce “Správa protokolů” na stránce 585 .

Soubory sekundárního protokolu

Ačkoli jsou sekundární soubory protokolů definovány pro lineární protokolování, nejsou použity v běžném provozu. Pokud se vyskytne situace, kdy, pravděpodobně kvůli dlouhodobým transakcím, není možné

uvolnit soubor z aktivního fondu, protože to může být stále potřeba pro restart, sekundární soubory jsou formátovány a přidány do aktivního fondu souborů protokolu.

Pokud je použit počet sekundárních souborů, které jsou k dispozici, požadavky na většinu dalších operací vyžadujících aktivitu protokolu budou odmítnuty s návratovým kódem MQRC_RESOURCE_PROBLEM vráceným do aplikace a všechny přerušitelné transakce budou zvažovány pro asynchronní odvolání transakce.

Upozornění: Oba typy protokolování se mohou vypořádat s neočekávanou ztrátou výkonu za předpokladu, že nedošlo k žádnému selhání hardwaru.

Použití kontrolního bodu k zajištění úplné obnovy

Jak kruhové protokolování, tak i správci front s lineárním protokolováním podporují opětovné spuštění zotavení. Bez ohledu na to, jak neočekávaně skončí předchozí instance správce front (například výpadek proudu) při restartu správce front, obnoví svůj trvalý stav do správného transakčního stavu v místě ukončení.

Restart obnovy závisí na zachování integrity disku. Podobně operační systém by měl zajistit integritu disku bez ohledu na to, jak nečekaně může dojít k ukončení operačního systému.

V případě velmi neobvyklé události, že integrita disku není udržována, poskytuje lineární protokolování (a obnova médií) další možnosti redundance a možností zotavení. Se stále více běžnými technologiemi, jako je RAID, je čím dál vzácnější a trpí problémy s integritou disků a mnoho podniků konfiguruje kruhové protokolování a používá pouze obnovu restartu.

IBM MQ je navržen jako klasický správce prostředků protokolování zápisu dopředu. Trvalé aktualizace front zpráv probíhá ve dvou fázích:

1. Záznamy protokolu představující aktualizaci jsou zapsány spolehlivě do protokolu pro zotavení
2. Soubor fronty nebo vyrovnávací paměti jsou aktualizovány způsobem, který je pro váš systém nejefektivnější, ale nemusí být nutně konzistentně konzistentní.

Soubory protokolu se tak mohou stát aktuálnější než základní vyrovnávací paměť fronty a stav souboru.

Pokud by tato situace mohla pokračovat, je třeba velmi velký objem přehrávání protokolu, aby byl stav fronty konzistentní po zotavení z havárie.

IBM MQ používá `checkpoints` , aby se omezil objem přehrávání protokolu, který se požaduje po zotavení z havárie. Klíčová událost, která řídí, zda je soubor protokolu označen jako aktivní nebo ne, je `checkpoint`.

Kontrolní bod IBM MQ je bod:

- Konzistentnosti mezi protokolem o zotavení a soubory objektů.
- To identifikuje místo v protokolu, z něhož je zaručeno přehrání následujících záznamů protokolu pro obnovení fronty do správného logického stavu v době, kdy mohl správce front skončit.

Během kontrolního bodu IBM MQ vyprázdní starší aktualizace do souborů fronty podle potřeby, aby bylo možné omezit objem záznamů žurnálu, které je třeba přehrát, aby se fronty vraly zpět do konzistentního stavu po obnově po havárii.

Poslední dokončený kontrolní bod označuje bod v protokolu, ze kterého musí být přehrán přehrání během zotavení z havárie. Frekvence kontrolního bodu je tedy odvoláním mezi režií záznamu kontrolních bodů a zvýšením potenciálního času obnovy odvozeného z těchto kontrolních bodů.

Pozice v protokolu spuštění posledního dokončovacího kontrolního bodu je jedním z klíčových faktorů pro určení, zda je soubor protokolu aktivní nebo neaktivní. Dalším klíčovým faktorem je pozice v protokolu prvního záznamu protokolu vztahující se k první trvalé aktualizaci provedené aktuální aktivní transakcí.

Je-li nový kontrolní bod zaznamenán ve druhém nebo novějším souboru protokolu a žádná aktuální transakce se neodkazuje na záznam protokolu v prvním souboru protokolu, první soubor protokolu se stane neaktivním. V případě kruhového protokolování je nyní první soubor protokolu připraven k opětovnému použití. V případě lineárního protokolování se první soubor protokolu obvykle požaduje pro obnovu médií.

Pokud nakonfigurujete buď kruhové protokolování, nebo automatickou správu protokolu, správce front bude spravovat neaktivní soubory protokolu. Pokud nakonfigurujete lineární protokolování pomocí ruční správy protokolů, stane se administrativní úlohou pro správu neaktivních souborů podle požadavků vaší operace.

Produkt IBM MQ generuje kontrolní body automaticky. Jsou převzaty v následujících případech:

- Při spuštění správce front
- Při ukončení práce
- Když je protokolovací prostor nízký
- Multi Po provedení předchozího kontrolního bodu bylo zaprotokolováno 50 000 operací.
- z/OS Po provedení *počet_operací* byly zaprotokolovány od posledního provedení kontrolního bodu, kde *počet_operací* je počet operací nastavených ve vlastnosti **LOGLOAD** .

Když se IBM MQ znovu spustí, najde v protokolu nejnovější záznam kontrolního bodu. Tyto informace jsou uloženy v souboru kontrolního bodu, který je aktualizován na konci každého kontrolního bodu. Všechny operace, k jejichž provedení došlo od kontrolního bodu, se přehrávají vpřed. To je známo jako fáze přehrání.

Fáze přehrávání vrací fronty zpět do logického stavu, ve kterém byly před selháním systému nebo ukončením běhu systému. Během fáze přehrávání je vytvořen seznam transakcí, které byly prolet při selhání systému nebo k ukončení práce systému.

Multi Vydávají se zprávy AMQ7229 a AMQ7230 , které označují průběh fáze přehrávání.

Chcete-li zjistit, které operace mají být odvraceny nebo potvrzeny, IBM MQ přistupuje ke každému aktivnímu záznamu protokolu přidruženému k transakci v rámci letu. Tento stav je znám jako fáze obnovení.

Multi Zprávy AMQ7231, AMQ7232 a AMQ7234 jsou vydávány s cílem označit průběh fáze obnovení.

Jakmile jsou k dispozici všechny potřebné záznamy protokolu během fáze obnovy, každá aktivní transakce se zase vyřeší a každá operace přidružená k transakci bude buď vrácena, nebo potvrzena. To je známo jako fáze řešení.

Multi Byla vydána zpráva AMQ7233 , která označuje průběh fáze rozpoznání.

z/OS V systému z/OSse zpracování restartu skládá z různých fází.

1. Rozsah protokolu pro zotavení je založen na obnově médií požadovaných pro sady stránek a na nejstaršímu záznamu protokolu, který je nezbytný pro zálohování jednotek práce a získání zámků pro nejisté jednotky práce.
2. Jakmile je určen rozsah protokolu, je dopředné čtení protokolu prováděno tak, aby stránka byla nastavena na nejnovější stav, a také uzamknout všechny zprávy související s neověřeným nebo neověřeným pracovním jednotkám.
3. Po dokončení dopředného čtení protokolů jsou protokoly čteny zpět, aby se vymkly veškeré jednotky práce, které byly v době selhání za letu nebo v době selhání.

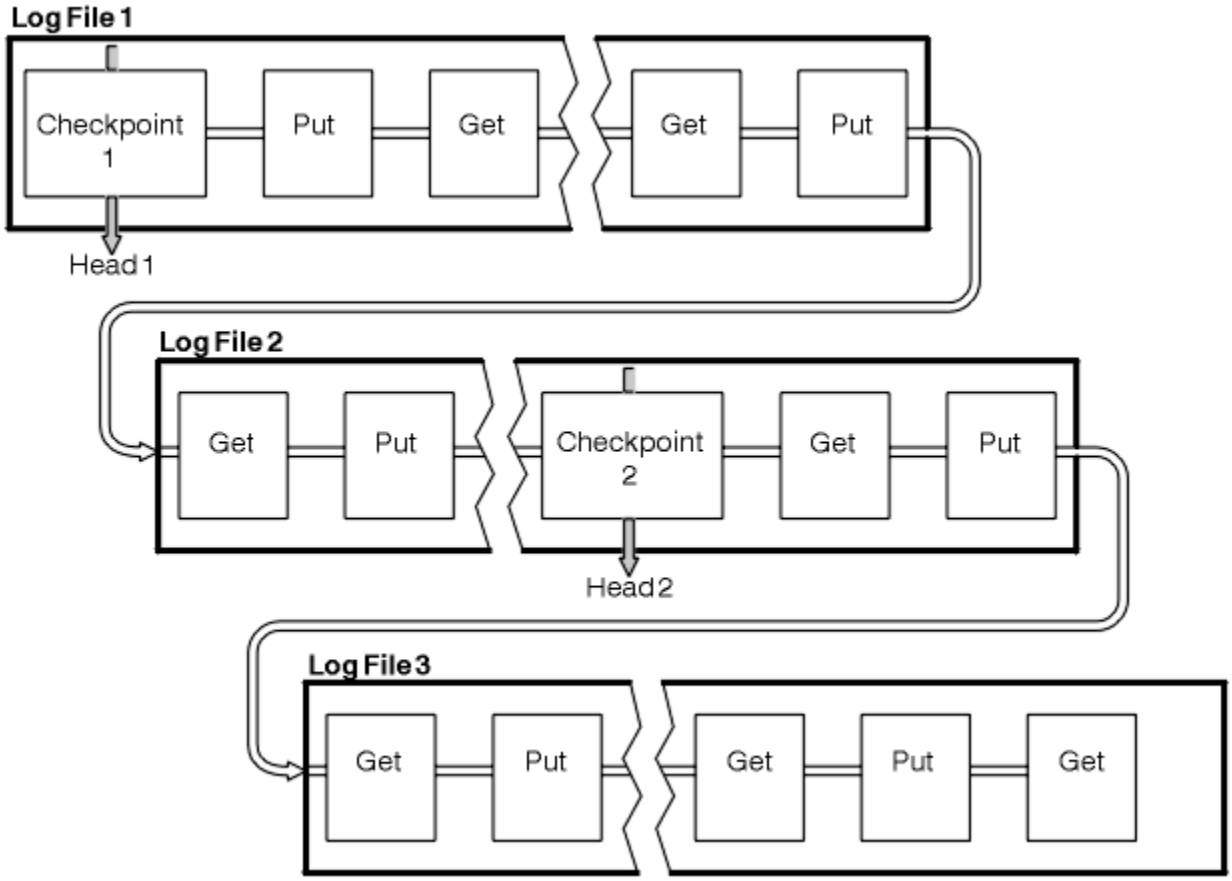
z/OS Příklad zpráv, které se mohou zobrazit:

```
CSQR001I +MQOX RESTART INITIATED
CSQR003I +MQOX RESTART - PRIOR CHECKPOINT RBA=00000001E48C0A5E
CSQR004I +MQOX RESTART - UR COUNTS -  806
IN COMMIT=0, INDOUBT=0, INFLIGHT=0, IN BACKOUT=0
CSQR030I +MQOX Forward recovery log range  815
from RBA=00000001E45FF7AD to RBA=00000001E48C1882
CSQR005I +MQOX RESTART - FORWARD RECOVERY COMPLETE -  816
IN COMMIT=0, INDOUBT=0
CSQR032I +MQOX Backward recovery log range  817
from RBA=00000001E48C1882 to RBA=00000001E48C1882
```

```
CSQR006I +MQOX RESTART - BACKWARD RECOVERY COMPLETE -  818
INFLIGHT=0, IN BACKOUT=0
CSQR002I +MQOX RESTART COMPLETED
```

Poznámka: Pokud existuje velké množství protokolu, které má být přečten, zprávy CSQR031I (dopředné zotavení) a CSQR033I (zpětné zotavení) jsou vydávány pravidelně pro zobrazení postupu.

V produktu Obrázek 86 na stránce 578již nejsou všechny záznamy před posledním kontrolním bodem, kontrolním bodem 2, již IBM MQvyžadovány. Fronty je možné obnovit z informací o kontrolním bodu a všech pozdějších položek protokolu. Pro kruhové protokolování se všechny uvolněné soubory před kontrolním bodem mohou znovu použít. V případě lineárního protokolu se uvolněné soubory protokolu již nemusí zpřístupnit pro normální provoz a stát se neaktivními. V tomto příkladu se ukazatel hlavy fronty přesune na poslední kontrolní bod kontrolního bodu 2, který se pak stane novou hlavou fronty, hlava 2. Soubor protokolu 1 lze nyní znovu použít.



Obrázek 86. Ukládám

Kontrola s dlouhotrvanými transakcemi

Jak dlouho běžící transakce ovlivňuje opětovné použití souborů protokolu.

Příkaz Obrázek 87 na stránce 579 zobrazuje, jak dlouho běžící transakce ovlivňuje opětovné použití souborů protokolu. V tomto příkladu provedla transakce s dlouhou dobou zpracování záznam do protokolu, zobrazený jako LR 1, po prvním zobrazení kontrolního bodu. Transakce se nedokončila (v bodě LR 2) až po třetím kontrolním bodu. Všechny informace z protokolu od LR 1 jsou uchovány, aby umožnily obnovu této transakce, je-li to nezbytné, dokud nebude dokončena.

Po dokončení transakce s dlouhou dobou zpracování v LR 2 se hlava protokolu logicky přesune do kontrolního bodu 3, nejnovější zaprotokolovaný kontrolní bod. Soubory obsahující záznamy protokolu před kontrolním bodem 3, hlava 2, již nejsou potřebné. Používáte-li kruhové protokolování, lze prostor znovu použít.

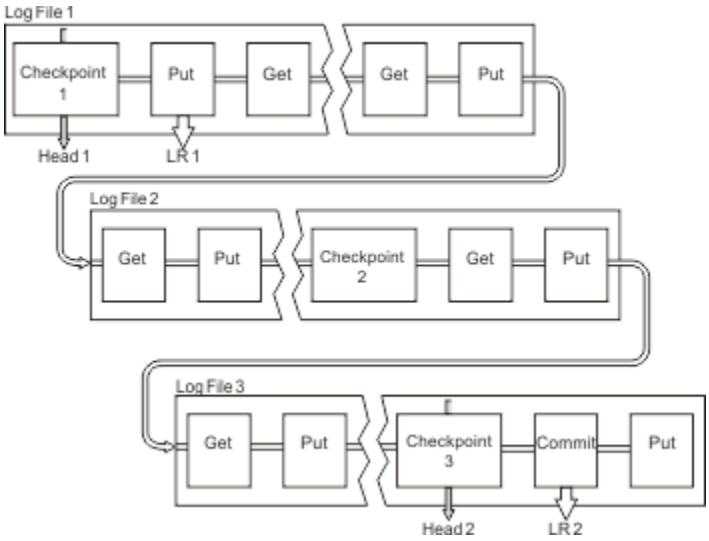
Pokud jsou primární soubory žurnálu zcela zaplněna před dokončením transakce s dlouhou dobou zpracování, mohou být použity sekundární soubory protokolu, aby nedošlo k zaplnění protokolů.

Aktivity, které jsou zcela pod kontrolou správce front, například checkpointing, jsou naplánovány, aby se pokusila udržet aktivitu v rámci primárního protokolu.

Je-li však pro podporu chování mimo kontrolu správce front vyžadován sekundární prostor žurnálu (například doba trvání jedné z vašich transakcí), správce front se pokusí použít definovaný sekundární protokolovací prostor, aby mohla být tato aktivita dokončena.

Pokud se tato aktivita nedokončí do doby, kdy se používá 80% celkového prostoru protokolu, správce front zahájí akci pro uvolnění protokolovacího prostoru bez ohledu na to, že má dopad na aplikaci.

Když se hlava protokolu přesune a používáte kruhové protokolování, mohou být primární soubory protokolu vhodné k opětovnému použití a modul protokolování po vyplnění aktuálního souboru znovu použije první primární soubor, který je k dispozici. Pokud používáte lineární protokolování, hlavička protokolu je stále přesunuta dolů do aktivního fondu a první soubor se stane neaktivní. Nový primární soubor je formátován a přidán do spodní části fondu v připravenosti pro budoucí aktivity protokolování.



Obrázek 87. Kontrola s dlouhotrvající transakcí

Výpočet velikosti protokolu

Odhadování velikosti protokolu, které správce front potřebuje.

Po rozhodnutí, zda správce front používá kruhové nebo lineární protokolování, je třeba odhadnout velikost Aktivní protokol , který správce front potřebuje. Velikost aktivního žurnálu se určuje podle následujících konfiguračních parametrů protokolu:

LogFilePages
Velikost každého primárního a sekundárního souboru protokolu v jednotkách stránek 4K

LogPrimaryFiles
Počet předem přidělených primárních souborů protokolu

LogSecondaryFiles
Počet sekundárních souborů protokolu, které lze vytvořit pro použití při zaplnění primárních souborů protokolu

Notes:

1. Můžete změnit počet primárních a sekundárních souborů protokolu při každém spuštění správce front, ačkoli si nemusíte všimnout efektu změny, kterou jste provedli na sekundárních protokolech, okamžitě.
2. Velikost souboru protokolu nelze změnit. Před vytvořením správce front je třeba určit **před** vytvořením správce front.

3. Počet primárních souborů protokolu a velikost souboru protokolu určují velikost prostoru protokolu, který je předem přidělen při vytvoření správce front.
4. Celkový počet primárních a sekundárních souborů protokolu nesmí překročit 511 na systémech UNIX and Linux nebo 255 na Windows, který za přítomnosti dlouho běžících transakcí omezuje maximální velikost protokolovacího prostoru dostupného správci front pro opětovné spuštění zotavení. Množství protokolovacího prostoru, které správce front potřebuje pro obnovu médií, tento limit nesdílí.
5. Je-li používáno *kruhové* protokolování, správce front znovu použije primární a sekundární protokolovací prostor. Správce front bude až do limitu alokovat sekundární soubor protokolu, když se soubor protokolu zaplní, a další primární soubor protokolu v posloupnosti nebude k dispozici.

   Informace o počtu protokolů, které je třeba přidělit, naleznete v příručce “Jak velký mám udělat svůj aktivní protokol?” na stránce 580 . Oblasti primárního protokolu se používají v pořadí a tato posloupnost se nezmění.

   Například, pokud máte tři primární protokoly 0, 1a 2, pořadí použití je 0,1,2 následované 1,2,0, 2,0,1, zpět na 0,1,2 atd. Všechny sekundární protokoly, které jste přidělili, jsou prosouzeni podle potřeby.
6. Primární soubory protokolu jsou k dispozici pro opětovné použití během kontrolního bodu. Před přijetím kontrolního bodu správce front vezme v úvahu jak primární, tak sekundární prostor žurnálu, protože velikost prostoru žurnálu je nízká.

   V 9.1.0 Správce front se pokusí naplánovat kontrolní body tak, aby zachovaly využití protokolu v rámci primárních fyzických oblastí.

Další informace viz “Sekce LogDefaults souboru mqs.ini” na stránce 91.

Jak velký mám udělat svůj aktivní protokol?

Odhadování velikosti aktivního protokolu, který správce front potřebuje.

Velikost aktivního žurnálu je omezena:

```
logsize = (primaryfiles + secondaryfiles) * logfilepages * 4096
```

Protokol by měl být dostatečně velký, aby se mohl vypořádat s nejdelší spuštěnou transakcí spuštěnou v okamžiku, kdy správce front zapisuje maximální množství dat za sekundu na disk.

Pokud vaše nejdelší běžící transakce běží na N sekund a maximální množství dat za sekundu zapsaných na disk správcem front je B bajtů za sekundu v protokolu, váš protokol by měl být alespoň:

```
logsize >= 2 * (N+1) * B
```

Správce front bude pravděpodobně zapisovat maximální množství dat za sekundu na disk, pokud pracujete v pracovní zátěži, nebo může být při záznamu obrazů médií.

Pokud je transakce spuštěna tak dlouho, že oblast protokolu obsahující svůj první záznam protokolu není obsažena v aktivním protokolu, správce front odvolá aktivní transakce jeden po druhém, počínaje transakcí s nejstarším záznamem protokolu.

Správce front musí před použitím maximálního počtu primárních a sekundárních souborů deaktivovat staré oblasti pro rozšíření protokolu a správce front musí přidělit další oblast protokolu.

Rozhodněte se, jak dlouho má trvat nejdéle běžící transakce, než bude správce front povolen návrat zpět. Vaše nejdelší běžící transakce může čekat na pomalý provoz sítě nebo, v případě špatně navržené transakce, čekat na vstup uživatele.

Zadáním následujícího příkazu **runmqsc** můžete zjistit, jak dlouho se nejdéle běžící transakce spouští:

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

Vydáním příkazu `dspmqtrn -a` se zobrazí všechny příkazy XA a non XA ve všech stavech.

Vydáním tohoto příkazu vypíše datum a čas, kdy byl zapsán první záznam protokolu pro všechny vaše aktuální transakce.

Upozornění: Pro účely výpočtu velikosti protokolu se jedná o čas od okamžiku, kdy byl zapsán první záznam protokolu, a nikoli čas od spuštění aplikace nebo transakce. Zaokrouhlit délku nejdéle běžící transakce na nejbližší sekundu. Je to způsobeno optimalizací ve správci front.

První záznam protokolu může být zapsán dlouho po spuštění aplikace, pokud aplikace začíná například zadáním volání MQGET, které čeká po určitou dobu, než se skutečně dostane zprávy.

Přezkoumáním maximálního sledovaného data a času výstupem z

```
DISPLAY CONN(*) UOWLOGDA UOWLOGTI
```

command you issued originally, from the current date and time, you can estimate how long your long along running transaction runs.

Ujistěte se, že jste spustili tento příkaz **runmqsc** opakovaně, zatímco nejdéle běžící transakce jsou spuštěny ve špičce pracovní zátěže, abyste nepodceňovali délku nejdelší spuštěné transakce.

V produktu IBM MQ 8.0 lze používat nástroje operačního systému, například **iostat** na platformách UNIX .

V produktu IBM MQ 9.0můžete zjistit počet bajtů za sekundu, které správce front zapisuje do protokolu, zadáním následujícího příkazu:

```
amqsrua -m qmgr -c DISK -t Log
```

Počet zapsaných logických bajtů zobrazuje počet bajtů 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
```

ukázala, že nejdelší běžící transakce byla:

```
CONN(57E14F6820700069)
EXTCONN(414D51436D61726B2020202020202020)
TYPE(CONN)
APPLTAG(msginteg_r)                     UOWLOGDA(2016-09-20)
UOWLOGTI(16.44.14)
```

Jako aktuální datum a čas byl 2016-09-20 16.44.19, tato transakce byla spuštěna po dobu 5 sekund. Je však nutné tolerovat transakce trvající 10 sekund, než je správce front odvolá zpět. Velikost protokolu by proto měla být následující:

```
2 * (10 + 1) * 12 = 264 MiB
```

.

Počet souborů protokolu musí být schopen obsahovat největší očekávanou velikost protokolu (vypočtenou v předchozím textu). To bude:

Minimální počet souborů protokolu = (požadovaná velikost protokolu)/(**LogFilePages** * velikost stránky souboru protokolu (4096))

Při použití výchozího nastavení **LogFilePages**, který je 4096, a odhad velikosti protokolu 264MiB, vypočteného v předchozím textu, by měl být minimální počet souborů protokolu:

```
264MiB / (4096 x 4096) = 16.5
```

To je, 17 souborů protokolu.

Pokud velikost protokolu zadáte tak, aby se očekávaná pracovní zátěž spouštělo v rámci primárních souborů, postupujte takto:

- Sekundární soubory poskytují určitou rezervu v případě, že je potřeba dodatečný prostor protokolu.
- Kruhové protokolování vždy používá předem přidělené primární soubory, což je okrajově rychlejší než přidělování a dealokace sekundárních souborů.
- Správce front používá pouze zbývající prostor v primárních souborech k výpočtu, kdy má být použit další kontrolní bod.

Proto v předchozím příkladu nastavte následující hodnoty tak, aby se pracovní zátěž spouštěla v rámci primárních souborů protokolu:

- **LogFilePages** = 4096
- **LogPrimaryFiles** = 17
- **LogSecondaryFiles** = 5

Všimněte si následujícího:

- V tomto příkladě 5 sekundářů je o více než 20% aktivního protokolovacího prostoru.

  V 9.1.0 V produktu IBM MQ 9.1.0se modul protokolování pokouší udržet pracovní zátěž pouze v primárních souborech. Proto modul protokolování naplánuje kontrolní body, když je plný pouze zlomek z primárních souborů.

  V 9.1.0 Sekundární soubory jsou nepředvídané události, v případě neočekávaných dlouho běžících transakcí.

  Měli byste si být vědomi toho, že správce front podničí kroky ke snížení využití protokolovacího prostoru, pokud se používá více než 80% celkového prostoru protokolu.
- Proveďte stejný výpočet, ať už používáte lineární nebo kruhové protokolování.

  Nezáleží na tom, zda vypočítáte velikost lineárního nebo kruhového aktivního protokolu, protože koncept aktivního protokolu znamená stejný jak v lineárním, tak i v kruhové protokolování.
- Oblasti protokolu potřebné pro obnovení médií nejsou v aktivním protokolu, a proto se nezapočítávají do počtu primárních a sekundárních souborů.
- V 9.1.0 Z IBM MQ 9.1.0 pole *LOGUTIL* příkazu DISPLAY QMSTATUS LOG je k dispozici, abyste mohli vypočítat, přibližně velikost aktivního protokolu.

  Toto pole je navrženo tak, aby umožňilo provádět přiměřený odhad požadované velikosti protokolu bez neustálého odebírání vzorků za účelem určení doby trvání nejdéle spuštěných transakcí nebo maximální propustnosti správce front.

Jak velký by měl být můj LogFileStránky?

Obecně platí, že vaše stránky LogFilejsou dostatečně velké, abyste mohli snadno zvýšit velikost aktivního protokolu, aniž byste dosáhli maximálního počtu primárních souborů. Několik velkých souborů protokolu je vhodnější pro mnoho malých souborů žurnálu, protože několik velkých souborů protokolu umožňuje větší flexibilitu při zvětšování velikosti protokolu, pokud potřebujete.

V případě lineárního protokolování mohou mít velmi velké soubory protokolu proměnnou výkonu. S velmi rozsáhlými soubory protokolů existuje větší krok k vytvoření a formátování nového souboru protokolu, nebo k archivaci starého souboru. Toto je spíše problém s manuálním a archivačním protokolem správy, protože s automatickým protokolem správy protokolů jsou zřídka vytvořeny nové soubory protokolu.

Co se stane, když udělám svůj protokol příliš malý?

Body, které byste měli zvážit při odhadu minimální velikosti protokolu.

Pokud je váš protokol příliš malý:

- Dlouho běžící transakce budou vráceny zpět.
- Další kontrolní bod se chce spustit dříve, než se předchozí kontrolní bod ukončí.

Důležité: Bez ohledu na to, jak přesně odhadujete velikost vašeho protokolu, zachovají se integrita dat.

Vysvětlení kontrolních bodů viz “Použití kontrolního bodu k zajištění úplné obnovy” na stránce 576 . Pokud se velikost protokolovacího prostoru, který zbývá v oblastech aktivního protokolu, stává krátkou, správce front naplánuje kontrolní body častěji.

Kontrolní bod zabere určitý čas; není okamžitý. Čím více dat je třeba zaznamenat do kontrolního bodu, tím déle bude kontrolní bod trvat. Pokud se protokol malých kontrolních bodů může překrývat, znamená to, že další kontrolní bod je požadován dříve, než skončí předchozí kontrolní bod. Pokud se tato chyba vyskytne, jsou zapsány chybové zprávy.

Pokud dojde k překryvu dlouhých spuštěných transakcí nebo se kontrolní body překrývají, bude správce front pokračovat ve zpracování pracovní zátěže. Krátkodobé transakce jsou nadále spuštěné jako normální.

Správce front však není spuštěn optimálně a výkon může být snížen. Měli byste restartovat správce front s dostatkem protokolovacího prostoru.

Co se stane, pokud se můj protokol příliš velký?

Body, které byste měli zvážit při odhadu maximální velikosti protokolu.

Pokud je váš protokol příliš velký:

- Můžete zvýšit čas potřebný k nouzovému restartu, i když je to nepravděpodobné.
- Používáte zbytečný prostor na disku.
- Velmi dlouho trvající transakce jsou tolerovány.

Důležité: Bez ohledu na to, jak přesně odhadujete velikost vašeho protokolu, zachovají se integrita dat.

V 9.1.0 Pro odhadování maximální velikosti protokolu můžete použít statistiku využití protokolu. Další informace viz “Rozhodování o tom, jak nastavit IMGLOGLN a IMGINTVL” na stránce 589 a ALTER QMGR.

Popis způsobu, jakým správce front čte protokol při restartování, naleznete v tématu “Použití kontrolního bodu k zajištění úplné obnovy” na stránce 576 . Správce front přehraje protokol z posledního kontrolního bodu a poté vyřeší všechny transakce, které byly aktivní v okamžiku, kdy byl ukončen správce front.

Při řešení transakce správce front načte zpět všechny záznamy protokolu přidružené k dané transakci. Tyto záznamy protokolu mohou přededat poslední kontrolní bod.

Při přidělení velmi rozsáhlého protokolu správce front přidělujete správci front oprávnění ke čtení každého záznamu žurnálu v protokolu při restartu, ačkoli obvykle správce front toto nemusí provést. Potenciálně, v nepravděpodobném případě, že by se to stalo, tento proces by mohl trvat dlouho.

Pokud před ukončením správce front došlo k neočekávanému ukončení kontroly před koncem správce front, výrazně se prodlužuje doba restartování správce front s velkým protokolem. Omezení velikosti protokolu omezuje dobu spuštění nouzového restartu.

Abyste se vyhnuli těmto problémům, měli byste zajistit, že:

- Vaše pracovní zátěž se může pohodlně vejít do protokolu, který není příliš velký.
- Vyhýbejte se přerušitelných transakcích.

V 9.1.0 *Jak velká by se měla vytvořit systém souborů protokolu?*

Odhadování velikosti systému souborů protokolu, které potřebuje správce front.

Je důležité, aby systém souborů protokolu byl dostatečně velký, aby měl správce front dostatek prostoru pro zápis svého protokolu. Pokud správce front zcela zaplní systém souborů protokolu, bude zapisovat FFDC, transakce odvolání transakce a může neočekávaně ukončit správce front.

Množství místa na disku, které rezervujete pro protokol, musí být alespoň tak velké jako aktivní protokol. Přesně, jak mnohem větší závisí na:

- Vaše volba typu protokolu (lineární nebo kruhové)
- Velikost aktivního protokolu (primární soubory, sekundární soubory, stránky souboru protokolu)
- Váš výběr správy protokolů (ruční, automatické nebo archivační)
- Vaše pohotovostní plány v případě poškozeného objektu.

Pokud zvolíte cyklický protokol, pak by měl být váš systém souborů protokolu

```
LogFilesystemSize >= (PrimaryFiles + SecondaryFiles + 1) * LogFileSize
```

To umožní správci front zapisovat do všech primárních a sekundárních souborů. Za výjimečných okolností může správce front zapsat větší fyzickou oblast mimo počet sekundárních serverů. Tento algoritmus bere v úvahu předchozí algoritmus.

Vyberete-li lineární protokol, měl by být systém souborů protokolu výrazně větší než aktivní protokol.

Pokud vyberete ruční správu protokolu, správce front bude nadále zapisovat do nových oblastí protokolu, protože je potřebuje, a je vaší odpovědností je odstranit (a archivovat je), pokud již nejsou potřeba.

Čím větší je třeba, aby systém souborů protokolu byl do značné míry závislý na vaší strategii odstranění nadbytečných nebo neaktivních oblastí.

Můžete se rozhodnout archivovat a odstranit fyzické oblasti, jakmile se stanou neaktivními (nejsou potřeba pro obnovu po restartu), nebo se můžete rozhodnout archivovat a odstranit pouze nadbytečné fyzické oblasti (nepotřebné pro médium nebo restart obnovy).

Pokud archivujete a odstraňujete pouze nadbytečné fyzické oblasti a máte-li poškozený objekt, příkaz **MEDIALOG** se nebude přesouvat vpřed, takže se žádné další fyzické oblasti nepřestanou nadbytečnými. Chcete-li problém vyřešit, zastavte archivaci a odstraňování fyzických oblastí, například obnovením objektu.

Pokud pracovní zátěž nezastavíte, kolik času budete muset vyřešit, závisí na velikosti vašeho systému souborů protokolu. Proto je nejlepší mít při použití lineárního protokolování velkorysý systém souborů protokolu.

Vyberete-li lineární protokol a automatickou správu nebo správu protokolu archivace, správce front znovu použije fyzické oblasti protokolu.

Oblasti protokolu, které jsou k dispozici pro opětovné použití, mají předponu s písmenem R. Je-li obraz média zaznamenán, protože nadbytečné fyzické oblasti jsou archivovány, může správce front tyto oblasti znovu použít.

Znovupoužití oblastí pro rozšíření je tedy menší než délka dat zapsaných do protokolu mezi obrazy média:

```
ReuseExtents <= LogDataLengthBetweenMediaImages
```

Při automatickém záznamu obrazů médií a nastavení **IMGLOGLN**může být `LogDataLengthBetweenMediaImages` stejně jako dvojnásobek **IMGLOGLN** , protože **IMGLOGLN** je cíl, nikoli pevné maximum.

Při ručním záznamu obrazů médií nebo jejich zaznamenávání automaticky intervalem `LogDataLengthBetweenMediaImages` závisí na pracovní zátěži a intervalu mezi převzetím obrazů.

Kromě aktivních oblastí pro rozšíření a opětovného použití existují neaktivní fyzické oblasti (potřebné pouze pro obnovení médií) a nadbytečné fyzické oblasti (nejsou potřebné pro restart nebo zotavení média).

Při použití automatické správy nebo archivace správy protokolu správce front nepoužívá znovu fyzické oblasti, které jsou potřebné pro obnovení médií. Takže počet neaktivních oblastí pro rozšíření závisí na tom, jak často provádíte obrazy médií, a zda je berete ručně nebo automaticky.

IMGINTVL a **IMGLOGLN** jsou cíle, nikoli pevné minimum nebo maximum mezi obrazy média. Avšak při odhadování maximální velikosti systému souborů protokolu, které možná budete potřebovat, je nepravděpodobné, že by automatické obrazy médií byly zaznamenávány více než dvakrát **IMGINTVL** nebo **IMGLOGLN** .

Při nastavení velikosti systému souborů protokolu pomocí automatické správy nebo archivace správy protokolu byste měli zvážit, co se může stát, pokud je fronta nebo jiný objekt poškozen. V takovém případě není správce front schopen přijmout obraz média poškozeného objektu a produkt **MEDIALOG** se nebude posouvat vpřed.

Bude-li pracovní zátěž pokračovat, bude neaktivní protokol zvětšen a nelze jej znovu použít, protože nejstarší fyzická oblast potřebná pro zotavení média je stále potřebná a nelze ji znovu použít. Pokud bude pracovní zátěž pokračovat, budete mít až do úplného zaplnění systému souborů protokolu tento problém, než správce front zahájí odvolání transakcí a může dokonce náhle skončit.

Proto pro automatickou a archivační správu protokolů:

```
LogFilesystemSize > (PrimaryFiles + SecondaryFiles +
(((TimeBetweenMediaImages *2) + TimeNeededToResolveDamagedObject) * ExtentsUsedPerHour))
* LogFilePages
```

Poznámka: Předchozí algoritmus předpokládá, že je volána **SET LOG ARCHIVED** pro každou fyzickou oblast, jakmile již není potřeba pro zotavení média, pro správu archivního protokolu.

Správa protokolů

V 9.1.0 Od IBM MQ 9.1.0 IBM MQ 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 9.1.0 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

Komponenta protokolování správce front se může vypořádat s celým diskem a s úplnými soubory protokolu. Pokud se disk obsahující protokol zaplní, vydá správce front zprávu AMQ6709 a provede se záznam o chybě.

Soubory protokolu se vytvářejí ve své pevné velikosti a nejsou rozšířeny, aby se do nich zapisovány záznamy protokolu. To znamená, že produkt IBM MQ může nedostatek prostoru na disku spustit pouze v případě, že vytváří nový soubor. Při zápisu záznamu do protokolu nemůže dojít k nedostatku místa. Produkt IBM MQ vždy ví, kolik místa je k dispozici v existujících souborech protokolu, a spravuje prostor v souborech odpovídajícím způsobem.

V 9.1.0 Když v produktu IBM MQ 9.1.0používáte lineární protokolování, máte možnost použít:

- Automatická správa fyzických 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 ovládající použití obrazů médií.

  Další informace naleznete v popisu příkazu ALTER QMGR a ALTER QUEUES :

  – IMGINTVL
  – IMGLOGLN
  – IMGRKODO
  – IMGRCOVQ.
  – IMGSCHED

Kruhové protokolování vrací problém prostředku.

Pokud stále dochází k nedostatku místa, zkontrolujte, zda je konfigurace protokolu v konfiguračním souboru správce front správná. Je možné, že budete moci snížit počet primárních nebo sekundárních souborů protokolu, aby protokol nevyrostl z dostupného místa.

Velikost souborů protokolu pro existujícího správce front nelze změnit. Správce front vyžaduje, aby všechny oblasti žurnálu byly stejné velikosti.

Správa souborů protokolu

Alokujte dostatečný prostor pro vaše soubory protokolů. Pro lineární protokolování můžete odstranit staré soubory protokolu, když již nejsou potřeba.

Informace specifické pro kruhové protokolování

Používáte-li kruhové protokolování, ujistěte se, že je dostatek místa pro uchování souborů protokolu při konfiguraci systému (viz “Sekce LogDefaults souboru mqs.ini” na stránce 91 a “Sekce protokolu souboru qm.ini” na stránce 122). Množství prostoru na disku použitého protokolem se nezvýší za nakonfigurovanou velikost, včetně prostoru pro sekundární soubory, které mají být vytvořeny, když je to požadováno.

Informace specifické pro lineární protokolování

Pokud používáte lineární protokol, soubory protokolu se přidávají průběžně, když jsou protokolována data, a velikost použitého prostoru na disku se zvyšuje s časem. Je-li rychlost protokolovaných dat vysoká, prostor na disku se rychle používá v nových souborech protokolu.

V průběhu času se starší soubory protokolu pro lineární protokol již nemusí restartovat správce front nebo provést obnovu médií s jakýmikoli poškozenými objekty. Následující metody určují, které soubory protokolu se stále požadují:

Zprávy událostí modulu protokolování
Když se vyskytne významná událost, například obraz záznamu média, zprávy událostí modulu protokolování se generují. Obsah zpráv událostí modulu protokolování uvádí soubory protokolu, které jsou stále vyžadovány pro restart správce front, a zotavení média. Další informace o zprávách událostí modulu protokolování naleznete v tématu Události modulu protokolování .

Stav správce front
Spuštěním příkazu MQSC, DISPLAY QMSTATUS nebo PCF, Inquire Queue Manager Status, získáte informace o správci front, včetně podrobností o požadovaných souborech protokolu. Další informace o příkazech MQSC najdete v tématu Administrace pomocí příkazů MQSCa informace o příkazech PCF najdete v tématu Automatizace administrativních úloh.

Zprávy správce front
Správce front pravidelně vydává zprávy s dvojicí zpráv, které indikují, které soubory protokolu jsou potřeba:

- Zpráva AMQ7467I udává název nejstaršího souboru protokolu potřebného k restartování správce front. Tento soubor protokolu a všechny novější soubory protokolu musí být k dispozici během restartování správce front.
- Zpráva AMQ7468I uvádí název nejstaršího souboru protokolu potřebného pro zotavení média.

Chcete-li určit "starší" a "novější" soubory protokolu, použijte místo úpravy, které používá systém souborů, číslo souboru protokolu.

Informace vztahující se na oba typy protokolování

Jsou vyžadovány pouze soubory protokolu vyžadované pro restartování správce front, aktivní soubory protokolů, které jsou online. Neaktivní soubory protokolu lze zkopírovat na archivní médium, jako je například páska pro zotavení z havárie, a odebrat z adresáře protokolů. Neaktivní soubory protokolu, které nejsou povinné pro obnovu médií, mohou být považovány za nadbytečné soubory protokolu. Nepotřebné soubory protokolu můžete odstranit, pokud již nejsou pro vaši operaci zajímavé.

Pokud nelze najít žádný potřebný soubor protokolu, vydá se zpráva AMQ6767E . Vytvořte soubor protokolu a všechny následné soubory protokolu dostupné pro správce front a zkuste operaci zopakovat.

Vyčištění oblastí čištění automaticky-pouze lineární protokolování

Z produktu IBM MQ 9.1.0 máte možnost použít automatickou správu oblastí s lineárním protokolem protokolu, které již nejsou zapotřebí pro obnovu.

Atribut **LogManagement** se používá ve stanze Log souboru qm.ini nebo pomocí IBM MQ Explorerk nastavení automatického řízení. Další informace viz “Sekce protokolu souboru qm.ini” na stránce 122.

Další informace o operaci protokolu a následujících příkazech pro použití protokolu naleznete v parametru LOG produktu **DISPLAY QMSTATUS** :

- RESET QMGR
- Nastavit protokol

Automatická instalace obrázků médií-pouze lineární protokolování

V 9.1.0

Z produktu IBM MQ 9.1.0 je celkový přepínač, který řídí, zda správce front automaticky zapisuje obrazy médií, výchozí nastavení toho, že přepínač nebyl nastaven.

Pomocí následujících atributů správce front můžete určit, zda k automatickému zobrazení médií dochází, a frekvenci procesu.

IMGSCHED
Určuje, zda správce front automaticky zapisuje obrazy médií.

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 těžká, a chcete se ujistit, že propustnost systému není ovlivněna zobrazením automatických obrazů médií, můžete dočasně vypnout zobrazování automatických médií nastavením **IMGSCHED***(MANUAL)*.

Server **IMGSCHED** můžete kdykoli přepnout během pracovní zátěže.

Upozornění: Produkt **MEDIALOG** nebude přesunut vpřed, pokud neobdržíte obrazy médií, takže je třeba buď archivovat fyzické oblasti, nebo se ujistěte, že máte dostatek místa na disku.

Můžete také řídit automatické a ruční obrazy médií pro další uživatelem definované objekty:

- Ověřovací informace
- Kanál
- Připojení klienta
- Modul listener
- Seznam názvů
- Proces
- Fronta aliasů
- Lokální fronta
- Služba
- Téma

U interních systémových objektů, jako je například katalog objektů a objekt správce front, správce front automaticky zapisuje 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. Toto provedete pomocí atributu fronty produktu **IMGRCOVQ** .

Další informace o atributu **IMGRCOVQ** najdete v tématu ALTER QUEUES .

Notes:

1. Obrazy médií jsou podporovány pouze tehdy, když používáte lineární protokolování. Pokud jste aktivovali automatické obrazy médií, ale používají kruhové protokolování, je vydána chybová zpráva a atribut automatických obrazů médií správce front je vypnutý.
2. Pokud jste povolili automatické obrazy médií, ale neuvedli jste frekvenci, buď minuty, nebo megabajty protokolu, vydá se chybová zpráva a nepíší se žádné automatické obrazy médií.
3. Obraz média můžete ručně zaznamenat pomocí příkazu rcdmqimg , pokud jste nastavili **IMGSCHED***(AUTO)*, pokud chcete.

   To vám umožní provádět obrazy médií v době, která je vhodná pro váš podnik, například když je váš systém zticha. Při automatických snímcích médií se berou v úvahu tyto manuálové obrazy médií,

protože při manuálním snímkování média se obnovuje interval a délka protokolu, před kterým se převezme další automatický obraz média.

4. V produktu IBM MQ 9.1.0správce front zapisuje trvalé zprávy pouze v obrázcích médií, nikoli v přechodných zprávách. To může zmenšit velikost obrazů médií při migraci na IBM MQ 9.1.0 nebo pozdější

Rozhodování o tom, jak nastavit IMGLOGLN a IMGINTVL

V 9.1.0

Učinit **IMGLOGLN** a **IMGINTVL** dostatečně velké, takže správce front pouze utrácí zlomek času zaznamenávající média, ale dostatečně malý, takže:

- Poškozené objekty lze obnovit v přiměřeném časovém intervalu a
- Dost malé, aby se váš log zapadá na váš disk, aniž by došlo k nedostatku místa.

If you set **IMGLOGLN**, a good practice is to make **IMGLOGLN** many times the amount of data on your queues and many times the data rate of your workload. Čím větší je **IMGLOGLN**, tím méně času bude váš správce front zaznamenávat obrazy médií.

Podobně platí, že pokud nastavíte **IMGINTVL**, je dobrým zvykem **IMGINTVL** mnohokrát nastavit dobu, po kterou bude správce front zaznamenávat obraz média. Můžete zjistit, jak dlouho trvá nahrávat obraz média tím, že zaznamenáte jeden ručně.

Pokud uděláte **IMGLOGLN** a **IMGINTVL** příliš velkou, obnova poškozeného objektu může trvat velmi dlouho, protože všechny fyzické oblasti od posledního obrazu média se mají přehrát.

Učiňte **IMGLOGLN** a **IMGINTVL** dostatečně malý tak, aby byl maximální čas potřebný k obnově poškozeného objektu pro vás přijatelný.

Vytváření **IMGLOGLN** a **IMGINTVL** je velmi velké, znamená to, že protokol je velmi velký, protože obrazy médií jsou zaznamenány tak zřídka.

Upozornění: Ujistěte se, že se protokol této velikosti pohodlně vejde do vašeho systému souborů protokolů, protože vaše pracovní zátěž bude zálohována, pokud se systém souborů protokolu zcela zaplní.

Můžete nastavit jak **IMGINTVL** tak **IMGLOGLN**. To může být užitečné k tomu, aby bylo zajištěno pravidelné pravidelné obrazy médií během pracovní zátěže (řízené **IMGLOGLN**), ale občas jsou prováděny příležitostně, je-li pracovní zátěž velmi lehká (řízena produktem **IMGINTVL**).

IMGINTVL a **IMGLOGLN** jsou cíle pro interval a délku dat protokolu, mezi kterými jsou přijímána automatická média.

Tyto atributy by neměly být považovány za pevné maximum nebo minimum. Ve skutečnosti může správce front rozhodnout o naplánování automatického obrazu média dříve, pokud správce front zjistí, že je to opravdu dobrý čas:

- Vzhledem k tomu, že fronta je prázdná, je z hlediska výkonu nejhospodárnější, a proto je obraz média nejvýkonnější, a
- Obraz média nebyl zaznamenáván pro určitou dobu.

U příležitosti může být mezera mezi automatickými obrazy média o něco delší než buď, nebo obojí, **IMGINTVL** a **IMGLOGLN**.

Mezera mezi obrazy média může být větší než **IMGLOGLN** , pokud se množství dat ve frontách blíží k **IMGLOGLN**. Mezera mezi obrazy média může být větší než **IMGINTVL** , pokud trvá téměř tak dlouho jako **IMGINTVL** pro záznam obrazu média.

Jedná se o špatnou praxi, protože správce front by strávil velkou část 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 obrázky zvlášť pro každý objekt.

Postupně po čase se nahrává nahrání obrázků médií a místo toho se nahrává obrazy médií pro všechny objekty najednou. Toto časové rozložení se rozprostírá od dopadu nahrávacích obrazů médií a je další výhodou použití automatického záznamu obrázků médií při ručním nahrávání.

Ruční přidání obrazů médií-pouze lineární protokolování

V 9.1.0

Záznam obrazu média fronty zahrnuje zápis všech trvalých zpráv z této fronty do protokolu. Pro fronty obsahující velké objemy dat zpráv to zahrnuje zápis velkého množství dat do protokolu a tento proces může mít vliv na výkon systému, zatímco se to děje.

Zaznamenávání obrazů médií u jiných objektů bude pravděpodobně poměrně rychlé, protože obraz média jiných objektů neobsahuje uživatelská data.

Při zaznamenávání obrazů médií ve frontách je třeba pečlivě zvážit, aby proces nekolidoval s nejvyšší pracovní zátěží.

Musíte zaznamenat obraz média všech objektů pravidelně, aby bylo možné aktualizovat nejstarší oblast protokolu potřebnou pro obnovu média.

Dobrý čas pro záznam obrazu média fronty je, když je prázdný, protože v tomto bodě nejsou zapsána žádná data zprávy do protokolu. Naopak, špatný čas je, když je fronta velmi hluboká nebo má velmi velké zprávy na ní.

Dobrý čas na záznam obrazu média fronty je, když je váš systém tichý; že špatný čas je během špičkové pracovní zátěže. Je-li vaše pracovní zátěž vždy o půlnoci zticha, můžete se například rozhodnout, že zaznamenáte snímky médií o půlnoci každou noc.

Psací záznam každé z vašich front může šířit dopad na výkon, a tak snížit jeho účinek. Čím déle to bylo od doby, kdy jste naposledy zaznamenávali obrazy médií, tím důležitější je zaznamenat je, protože se zvyšuje počet oblastí protokolu požadovaných pro zotavení média.

Poznámka: Při provádění obnovení médií musí být všechny požadované soubory žurnálu dostupné v adresáři souborů protokolu v daném okamžiku. Ujistěte se, že jste provedli pravidelné obrazy médií u všech objektů, které byste mohli chtít obnovit, abyste se vyhnuli nedostatku místa na disku pro uchování všech požadovaných souborů protokolu.

Chcete-li například zobrazit obraz média všech objektů ve správci front, spusťte příkaz **rcdmqimg** , jak ukazuje následující příklady:

Windows **zapWindows**

```
rcdmqimg -m QMNAME -t all *
```

Linux UNIX **zapUNIX and Linux**

```
rcdmqimg -m QMNAME -t all "*"
```

Spuštění **rcdmqimg** přesune pořadové číslo v protokolu médií (LSN) dopředu. Další podrobnosti o pořadových číslech protokolů najdete v tématu “Výpis obsahu protokolu pomocí příkazu dmpmqlog” na stránce 597. **rcdmqimg** se nespustí automaticky, proto musí být spuštěn ručně nebo z automatické úlohy, kterou jste vytvořili. Další informace o tomto příkazu naleznete v části rcdmqimg a dmpmqlog.

Ruční záznam obrazů médií se systémem **rcdmqimg** pro správu prostoru protokolu není požadován, pokud jste zvolili použití lineárního protokolování se zobrazovaným automatickým zobrazováním médií správcem front.

Poznámka: Zprávy AMQ7467 a AMQ7468 lze také zadat v době spuštění příkazu `rcdmqimg` .

Částečné obrazy médií

V 9.1.0

Je dobrým zvykem používat zprávy produktu IBM MQ pouze pro data očekávaná v blízké budoucnosti, takže každá zpráva se nachází ve frontě relativně krátkou dobu.

Naopak je špatným zvykem používat zprávy produktu IBM MQ k ukládání dlouhodobých dat, jako je databáze.

Je také dobrým zvykem zajistit, aby vaše fronty byly relativně mělké a špatná praxe, aby měly hluboké fronty, jejichž zprávy byly ve frontě dlouhou dobu.

Podle těchto pokynů umožníte správci front optimalizovat výkon automatických záznamů obrazů médií.

Záznam obrazu média prázdné fronty je velmi účinný (z hlediska výkonu), zatímco při použití obrazu média fronty s velkým objemem dat je velmi neefektivní, protože všechna tato data musí být zapsána do protokolu v obrazu média.

U mělkých front s nedávnou zprávou o něm může správce front provést další optimalizaci.

Pokud byly všechny zprávy, které jsou momentálně ve frontě, vloženy do nedávné minulosti, může být správce front schopen zaznamenat obraz média za čas (*bod obnovy*) těsně před tím, než byly všechny zprávy vloženy, a tak být schopni zaznamenat obraz prázdné fronty. Tento proces je velmi nízký, pokud jde o výkon.

Pokud byly všechny zprávy, které byly ve frontě v bodu obnovy, následně získány, tyto zprávy nemusí být zaznamenány do obrazu média, protože již nejsou ve frontě.

Tomu se říká *částečný obraz média*. Poté v případě, že je fronta potřeba obnovit, budou všechny záznamy protokolů, které souvisí s touto frontou od posledního obrazu média, přehrány, takže obnoví všechny nedávno odeslané zprávy.

I když bylo na frontě několik zpráv v bodu obnovy, které jsou momentálně ve frontě (a tak musí být zaznamenány v částečném obrazu média), je stále efektivnější zaznamenat tento menší obrázek s částečným médiem, než je úplný obraz média všech zpráv.

Ujištění, že zprávy zůstanou ve frontách na krátkou dobu, je pravděpodobné, že se zlepší výkon automatického nahrávání obrazů médií.

Určení nadbytečných souborů protokolu-pouze lineární protokolování
Pro kruhové protokolování nikdy neodstraňujte data z adresáře protokolů. Při správě lineárních souborů protokolů je důležité si být jisti, které soubory mohou být odstraněny nebo archivovány. Tyto informace vám pomohou při provádění tohoto rozhodnutí.

Nepoužívejte čas úpravy systému souborů, abyste určili "starší" soubory protokolu. Použijte pouze číslo souboru protokolu. Použití souborů protokolu správce front je podle složitých pravidel, včetně předalokování a formátování souborů protokolu, dříve než je potřeba. Při pokusu o určení relativního stáří se mohou zobrazit soubory protokolu s časy úpravy, které by byly zavádějící.

K určení nejstaršího potřebného souboru žurnálu jsou k dispozici tři místa, která můžete použít:

- Příkaz DISPLAY QMSTATUS
- Zprávy událostí modulu protokolování a nakonec
- Zprávy protokolu chyb

Pro příkaz DISPLAY QMSTATUS určete nejstarší rozsah protokolu potřebný k:

- Restartujte správce front, zadejte příkaz `DISPLAY QMSTATUS RECLOG`.
- Proveďte obnovu médií, zadejte příkaz `DISPLAY QMSTATUS MEDIALOG`.
- V 9.1.0 Určete název pro oznámení o archivaci, zadejte příkaz `DISPLAY QMSTATUS ARCHLOG`.

V 9.1.0 Počet sekundárních fyzických oblastí protokolu můžete snížit při použití kruhové protokolování zadáním příkazu **RESET QMGR TYPE(REDUCELOG)**.

Obecně platí, že nižší číslo souboru protokolu znamená starší protokol. Pokud nemáte velmi vysoký obrat souboru protokolu, v pořadí 3000 souborů protokolu za den po dobu 10 let, nemusíte obstarávat balení čísel v 9 999 999. V tomto případě můžete archivovat libovolný soubor protokolu s číslem menším než hodnota RECLOG a můžete odstranit libovolný soubor protokolu s číslem menším, než je hodnota RECLOG a MEDIALOG.

Upozornění: The log file wraps, so the next number after 9 999 999 is zero.

Umístění souboru žurnálu
Při výběru umístění pro soubory protokolu pamatujte na to, že operace je výrazně ovlivněna, pokud produkt IBM MQ neformátuje nový protokol z důvodu nedostatku místa na disku.

Používáte-li cyklický protokol, ujistěte se, že na jednotce je dostatek místa pro alespoň konfigurované primární soubory protokolu. Také ponechejte prostor pro alespoň jeden sekundární soubor protokolu, který je potřebný, pokud má protokol růst.

Pokud používáte lineární protokol, umožněte výrazně více prostoru; prostor využitý protokolem se neustále zvyšuje, protože data jsou protokolována.

Měli byste umístit soubory protokolu na samostatnou diskovou jednotku z dat správce front.

Integrita dat na tomto zařízení je prvořadá-měli byste povolit zabudovanou redundanci.

Může být také možné umístit soubory protokolu na více diskových jednotek v zrcadleném uspořádání. To chrání před selháním jednotky, která obsahuje protokol. Bez zrcadlení byste mohli být nuceni vrátit se zpět k poslední záloze vašeho systému IBM MQ .

V 9.1.3 *Coldstart: Co dělat, pokud fyzické oblasti protokolu chybí nebo jsou poškozené*

Pokud váš podnik ztratí některé nebo všechny oblasti protokolu potřebné pro zotavení restartováním, nebude správce front moci přehrát protokol zotavení a nezdaří se restart. Pokud potřebujete restartovat správce front, je-li žurnál zotavení poškozen, a to na úkor zachování integrity dat, je to možné, ačkoli silně nedoporučujeme. Tento proces je znám jako *coldstarting* správce front.

Důležité: Coldstarting správce front by měl být považován za pouze za výjimečných okolností a nese rizika pro integritu dat, jak je popsáno na této stránce. Produkt IBMnavrhuje, abyste znovu sestavoval správce front v závislosti na tom, že jste začali pracovat s poškozenými datovými soubory, a to podle předvolby.

Je-li z provozních důvodů vyžadován sloupec coldstart, zapojte zástupce podpory IBM , abyste přezkoumali základní příčinu problému. Měli byste nahradit správce front Coldstarted novým správcem front při nejbližší příležitosti.

Efekty příkazu coldstart

Při spuštění sloupce coldstart vytvoří správce front prázdný protokol o zotavení a spoléhá na data v souborech fronty a na jiných souborech objektů v existujícím stavu. Vzhledem k tomu, že data v souborech fronty mohou být nekonzistentní, zprávy mohou být ztraceny, duplikovány, poškozeny nebo nekonzistentní.

Správce front ukládá konfiguraci všech ostatních trvalých objektů v protokolu pro zotavení a také v souborech objektů. Další vnitřní stavová data se také zaznamenávají do protokolu pro zotavení, takže na coldstart, data vnitřního stavu jsou resetována a všechna tato jiná konfigurační data mohou být nepřesná.

Účinky Coldstart jsou nepředvídatelné a pohybující se tak, že byste se měli vyhnout Coldstart, pokud absolutně nutné. Po spuštění příkazu coldstarting mohou být informace ve frontě a v souborech objektů tak nekonzistentní, že správce front nebude restartován vůbec.

Pokud se správce front restartuje, neexistuje žádný jednoduchý způsob, jak zjistit, jaká data zprávy nebo konfiguraci lze použít, a to, co nelze. Také po coldstart mohou být fronty poškozeny a tak se stanou zcela nepoužitelné.

Navíc, pokud se můžete dostat z určité fronty nebo ji vložit do určité fronty, zprávy na ní mohou být poškozené, chybějící nebo duplicitní. Transakce a kanály mohou být zablokované v nejistém stavu. I když se správce front úspěšně studuje a fronty vypadají neporušeně, nepředvídatelné účinky coldstart nemusí být realizováno až do mnohem vyšších hodnot.

Co dělat, pokud potřebujete provést Coldstart

Provedení Coldstart by nemělo být považováno za standardní operační postup a IBM vás odrazuje od toho, abyste to udělali. Avšak, pokud jste na místě, kde rozhodně potřebujete Coldstart zařadit správce front, kontaktujte IBM MQ Podpora .

Proces pro coldstarting správce front byl pro lineární správce front mnohem komplikovanější než cyklický správce front. V produktu IBM MQ 9.1.3byl proces coldstart velmi zjednodušený a nezahrnuje žádné další kopírování nebo přejmenování oblastí protokolu.

V produktu IBM MQ 9.1.3se obraťte na podporu produktu IBM , která vám předá klíč, který předáváte příkazu produktu **strmqm** ke spuštění správce front.

Upozornění: Příkaz coldstart produktu IBM MQ 9.1.3 stále nese stejná rizika jako ztráta integrity dat jako ruční coldstart, a produkt IBM vás odrazuje od toho, abyste to udělali.

Vyloučení budoucího studeného startu: žádost

Příkaz strmqm vyžaduje klíč k příkazu coldstart, protože produkt IBM MQ chce, abyste kontaktovali podporu produktu IBM MQ , pokud potřebujete provést Coldstart, protože produkt IBM MQ se snaží pochopit, jak jste se dostali do této situace.

Je zřejmé, že Coldstart je něco, co je nejlépe vyhnout. Produkt IBM MQ se vynasnažil vyvinout značné úsilí, aby se ujistil, že nebudete muset provést Coldstart vašeho správce front, a IBM se snaží zjistit, zda existuje něco více, co produkt může udělat, aby se zmírnil tím, že se Coldstart.

Opatření pro zamezení vzniku studeného startu

Výchozí metoda protokolování při vytváření správce front je kruhové protokolování. S kruhovým protokolováním umožníte správci front konkrétní počet primárních a sekundárních fyzických oblastí protokolu pro danou velikost. Vytvořte systém souborů protokolu dostatečně velký, aby obsahoval všechny primární a sekundární oblasti protokolu, a neměli byste je nikdy potřebovat spravovat.

Případně můžete použít lineární protokolování na rozdíl od kruhové. Lineární protokolování poskytuje přidanou schopnost obnovy front a jiných objektů, v nepravděpodobném případě, že dojde k jejich poškození. Při výchozím nastavení však lineární protokolování vyžaduje odstranění oblastí protokolu, které již nejsou potřebné k restartování nebo obnově médií. Tento postup je označován jako ruční správa protokolu.

Při správě oblastí protokolu tímto způsobem je možné nechtěně odstranit příliš mnoho oblastí protokolu a skončit tím, že se bude muset začít s Coldstart. Chcete-li toto riziko zmírnit, použijte automatickou správu protokolu, aby správce front spravoval fyzické oblasti protokolu ve vašem zastoupení.

Nejlepším postupem je umístění vašeho protokolu pro zotavení do samostatného systému souborů protokolu, který obsahuje pouze protokol zotavení. Pokud vložíte protokol zotavení do stejného systému souborů jako zbytek správce front, můžete někdy zjistit, že se systém souborů náhodně zaplnil, pravděpodobně kvůli rozsáhlým souborům fronty. Buď vytvořte adresář protokolu pro správce front jako samostatný systém souborů, nebo zadejte jiný systém souborů protokolu pomocí volby příkazového řádku **-ld** v příkazu **crtmqm** .

Pokud systém souborů, který je držitelem souborů fronty, se zaplní, nemusíte být schopni do těchto front vkládat, ale správce front bude i nadále pracovat. Pokud systém souborů, který obsahuje protokol pro zotavení, zaplní, správce front bude náhle ukončen a nebude restartován, dokud nebude uvolňovat prostor.

Je třeba dbát na to, aby nebyly odstraněny oblasti pro rozšíření protokolu potřebné pro opětovné spuštění zotavení, jinak může dojít k tomu, že budete muset začít Coldstart. Někdy možná zjistíte, že je třeba

provést Coldstart, protože disk selhal, který obsahuje protokol o zotavení. Doporučeným postupem je umístit žurnál zotavení na replikovaný disk a snížit tak riziko selhání disku.

Přesunutím vašich zpráv a konfigurace do nového náhradního správce front se vyhnete možnosti přetrvávajícím problémům se správcem front, který byl již dříve nachlazeného.

Mějte na paměti, že správci front byli již dříve spuštěni, a to i v případě, že byly před dlouhou dobou spuštěny a byly zastaveny, restartovány a migrovány do té doby. Když se obrátíte na podporu produktu IBM , řekněte, zda byl správce front již dříve spuštěn, a pokud ano, uveďte co nejvíce informací o tom, co způsobilo požadavek na coldstart.

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 se zotavit z:

- Poškozený datový objekt
- Ztráta napájení v systému
- Selhání komunikace

Tento oddíl se zabývá tím, jak se protokoly používají pro zotavení z těchto problémů.

Obnova ze výpadku proudu nebo selhání komunikace

Příkaz IBM MQ se může zotavit z obou selhání komunikace a ztráty moci. Může se také občas zotavit z jiných typů problémů, jako je například neúmyslné odstranění souboru.

V případě selhání komunikace zůstávají trvalé zprávy ve frontách, dokud nejsou odebrány přijímající aplikací. Je-li zpráva přenášena, zůstane v přenosové frontě, dokud ji nebude možné úspěšně přenést. Chcete-li provést obnovu po selhání komunikace, můžete obvykle restartovat kanály pomocí odkazu, který selhal.

If you lose power, when the queue manager is restarted IBM MQ restores the queues to their committed state at the time of the failure. Tím je zajištěno, že žádné trvalé zprávy nebudou ztraceny. Netrvalé zprávy jsou vyřazeny; nepřežijí, když se IBM MQ náhle zastaví.

Obnova poškozených objektů

Existují způsoby, jak může být objekt IBM MQ nepoužitelný, například z důvodu neúmyslného poškození. Pak musíte obnovit buď celý systém, nebo část jeho části. Požadovaná akce závisí na tom, kdy je poškození zjištěno, zda zvolená metoda protokolu podporuje obnovu médií a které objekty jsou poškozené.

Náprava média

V 9.1.0 Z produktu IBM MQ 9.1.0lze ve správci front s lineárním protokolováním zaznamenávat obrazy médií pouze pro objekty, které jsou obnovitelné. Například je třeba zvážit volby **IMGRCOVO** a **IMGRCOVQ** .

V 9.1.0 Podobně můžete obnovit podmnožinu objektů pouze, definovaných jako obnovitelná média, z jejich obrazů médií na správci front s lineárním protokolováním. V případě poškození objektu, který není definován jako opravitelná média, jsou volby pro tento objekt stejné jako volby pro správce front s kruhovým protokolováním.

Náprava médií znovu vytváří objekty z informací zaznamenaných v lineárním protokolu. Pokud je například soubor objektu neúmyslně odstraněn nebo je z nějakého jiného důvodu nepoužitelný, obnova média ji může znovu vytvořit. Informace v protokolu, které se požadují pro obnovu médií objektu, se nazývají *obraz média*.

Obraz média je posloupnost záznamů protokolů, které obsahují obraz objektu, ze kterého lze znovu vytvořit objekt.

První záznam protokolu požadovaný pro opětovné vytvoření objektu je známý jako *záznam o obnově médií* ; je to začátek posledního obrazu média pro objekt. Záznam obnovy médií každého objektu je jednou z částí informací zaznamenaných během kontrolního bodu.

Když je objekt znovu vytvořen z obrazu média, je také nutné přehrát všechny záznamy protokolu popisující aktualizace provedené na objektu od doby, kdy byl naposledy proveden.

Vezměme si například lokální frontu, která má obraz objektu fronty, který byl proveden před tím, než je do fronty vložena trvalá zpráva. Chcete-li znovu vytvořit nejnovější obraz objektu, je třeba přehrávat záznamy protokolu zaznamenávající vložení zprávy do fronty spolu s opětovným přehráváním obrazu.

Když je objekt vytvořen, záznamy v protokolu obsahují dostatek informací k úplnému znovuvytvoření objektu. Tyto záznamy tvoří první obraz média objektu. Poté správce front při každém vypnutí automaticky provede následující záznamy v obrázcích médií:

- Obrázky všech objektů procesu a front, které nejsou lokální
- Obrázky prázdných lokálních front

Obrazy médií lze také zaznamenat ručně pomocí příkazu **rcdmqimg** , který je popsán v souboru rcdmqimg. Tento příkaz zapíše obraz média objektu IBM MQ .

V 9.1.0 Správce front zaznamenává obrázky v médiích automaticky, pokud je nastavena hodnota **IMGSCHED***(AUTO)* . Další informace viz ALTER QMGR pro informace o **IMGINTVL** a **INGLOGLN**.

Když byl obraz média zapsán, jsou pro opětovné vytvoření poškozených objektů potřeba pouze protokoly, které obsahují obraz média a všechny protokoly vytvořené po této době. Přínos vytváření obrazů médií závisí na takových faktorech jako na množství volné paměti a rychlosti, jakou jsou soubory protokolu vytvořeny.

Obnova z obrazů médií

Správce front automaticky obnoví některé objekty ze svého obrazu média během spuštění správce front. Zotavuje frontu automaticky, pokud byla zahrnuta do transakce, která byla nekompletní, když správce front byl naposledy ukončen, a během restartu byl nalezen poškozený nebo poškozený.

Ostatní objekty je třeba obnovit ručně pomocí příkazu **rcrmqobj** , který přehraje záznamy v protokolu k opětovnému vytvoření objektu IBM MQ . Objekt je znovu vytvořen z jeho posledního obrazu nalezeného v protokolu, spolu se všemi příslušnými událostmi protokolu mezi časem, kdy byl obraz uložen, a časem, kdy byl vydán příkaz k vytvoření nového vydání. Je-li objekt IBM MQ poškozen, jediné platné akce, které lze provést, jsou buď pro její odstranění, nebo pro opětovné vytvoření této metody. Netrvalé zprávy nelze tímto způsobem obnovit.

Další podrobnosti o příkazu **rcrmqobj** naleznete v souboru rcrmqobj .

Soubor protokolu, který obsahuje záznam o obnově médií a všechny následné soubory protokolu, musí být k dispozici v adresáři souborů protokolu při pokusu o obnovení médií objektu. Pokud požadovaný soubor nelze najít, je vydána zpráva AMQ6767 a operace zotavení média selže. Pokud nevezmete pravidelné média s obrazy objektů, které chcete znovu vytvořit, můžete mít nedostatečný prostor na disku pro uchování všech souborů protokolu potřebných pro opětovné vytvoření objektu.

Jaké soubory objektů existují

V 9.1.0

Správce front ukládá atributy objektů, které jsou definovány v produktu **runmqsc** , v souborech na disku. Tyto objektové soubory jsou umístěny v podadresářích pod datovým adresářem správce front.

Linux UNIX Například na platformách UNIX a Linux jsou kanály uloženy v produktu `/var/mqm/qmgrs/qmgr/channel`.

Data v těchto souborech objektů jsou obrazem média objektů. Pokud jsou tyto soubory objektu odstraněny nebo poškozeny, objekt uložený v tomto souboru je poškozen. Pomocí správce front s lineárním protokolováním lze z protokolu zotavit poškozené objekty pomocí příkazu rcrmqobj .

Většina objektových souborů obsahuje pouze atributy objektu, takže soubory kanálů obsahují atributy kanálů. Výjimky jsou:

- Katalog

  Katalog objektů katalogizuje všechny objekty všech typů a je uložen v produktu `qmanager/QMQMOBJCAT`.

- Soubory Syncfile

  Synchronizační soubor obsahuje interní stavová data přidružená ke všem kanálům.

- Fronty

  Soubory fronty obsahují jak zprávy v této frontě, tak i atributy této fronty.

Povšimněte si, že v produktu **runmqsc** nebo v IBM MQ Explorernení vystaven žádný katalog nebo objekt syncfile.

Katalogový katalog a správce front lze zaznamenat, ale nikoli obnovit. Pokud se tyto objekty poškodí, ukončí správce front preemptivně a tyto objekty budou automaticky obnoveny při restartu.

Odběry nejsou uvedeny v objektech k záznamu nebo obnově, protože trvalé odběry jsou uloženy ve frontě systému. Chcete-li zaznamenat nebo obnovit trvalé odběry, zaznamenejte nebo obnovte SYSTEM.DURABLE.SUBSCRIBER.QUEUE .

Obnova poškozených objektů během spouštění

Pokud správce front zjistí poškozený objekt během spouštění, závisí akce na typu objektu a na tom, zda je správce front konfigurován tak, aby podporoval zotavení z médií.

Pokud je objekt správce front poškozen, správce front se nemůže spustit, pokud jej nemůže obnovit. Je-li správce front konfigurován s lineárním protokolem, a tak podporuje obnovu médií, produkt IBM MQ se automaticky pokusí znovu vytvořit objekt správce front z jeho obrazů médií. Pokud vybraná metoda protokolu nepodporuje zotavení média, můžete buď obnovit zálohu správce front, nebo odstranit správce front.

Pokud byly při zastavení správce front aktivní nějaké transakce, lokální fronty obsahující trvalé a nepotvrzené zprávy, které byly vloženy do těchto transakcí nebo se dostaly do těchto transakcí, jsou rovněž nezbytné ke spuštění správce front. Pokud se zjistí, že se některé z těchto lokálních front poškodí, a správce front podporuje obnovu médií, pokusí se je automaticky znovu vytvořit z jejich obrazů médií. Pokud některou z front nelze obnovit, nelze spustit příkaz IBM MQ .

Jsou-li během zpracování spuštění ve správci front, který nepodporuje obnovu médií, zjištěny jakékoliv poškozené lokální fronty obsahující nepotvrzené zprávy, fronty se označí jako poškozené a budou ignorovány nepotvrzené zprávy. Tato situace je, protože není možné provést obnovu médií poškozených objektů na takovém správci front a jediná akce, která zbývá, je odstranit je. Byla vydána zpráva AMQ7472 , která hlásí jakoukoli škodu.

Obnova poškozených objektů v jiných časech

Obnova médií objektů je automatická pouze během spouštění. V jiných případech je při zjištění poškození objektu vydána zpráva operátora AMQ7472 a většina operací s použitím objektu se nezdaří. Je-li objekt správce front poškozen v libovolném okamžiku po spuštění správce front, provede správce front preventivní ukončení. Když je objekt poškozen, můžete jej vymazat nebo, pokud správce front používá lineární protokol, pokuste se jej obnovit z obrazu svých médií pomocí příkazu **rcrmqobj** (další podrobnosti viz rcrmqobj).

V 9.1.0 Pokud dojde k poškození fronty (nebo jiného objektu), produkt **MEDIALOG** se nepřesune vpřed. Důvodem je to, že **MEDIALOG** je nejstarší oblastí, která je vyžadována pro zotavení média. Pokud vaše pracovní zátěž pokračuje, **CURRLOG** se stále přesune kupředu, a tak budou zapsány nové oblasti pro rozšíření. V závislosti na konfiguraci (včetně nastavení produktu **LogManagement**) může dojít k zaplnění systému souborů protokolu. Pokud se systém souborů protokolu zaplní, transakce se vrátí zpět a správce front může náhle skončit. Když se tedy fronta poškodí, může dojít k tomu, že budete mít před ukončením

správce front pouze omezené množství času. Doba, jakou máte, závisí na rychlosti, jakou pracovní zátěž způsobuje zápis nových oblastí, a množství volného místa, které máte ve svém systému souborů protokolu.

V 9.1.0 Pokud používáte ruční správu protokolů, můžete archivovat oblasti, které nejsou potřebné pro obnovení restartu, a pak je odstranit ze systému souborů protokolu, i když jsou stále potřebné pro zotavení média. To je přijatelné, pokud je v případě potřeby můžete obnovit z archivu. Tato zásada nezpůsobí, že se systém souborů protokolu zaplní, když dojde k poškození fronty a **MEDIALOG** přestane přesouvat vpřed. Pokud však archivujete a odstraňujete pouze fyzické oblasti, které nejsou potřebné k restartování nebo obnově médií, systém souborů protokolu se začne vyplňovat, pokud dojde k poškození fronty.

V 9.1.0 Pokud používáte automatickou nebo archivační správu protokolu, správce front nebude znovu používat fyzické oblasti, které jsou stále potřebné pro zotavení z médií, i když jste je mohli archivovat a oznámit správci front pomocí příkazu SET LOG ARCHIVED. V důsledku toho dojde k zaplnění fronty při poškození vašeho systému souborů s protokolem.

V 9.1.0 Pokud dojde k poškození fronty, dojde k zápisu záznamů FFDC produktu OBJECT DAMAGED a **MEDIALOG** přestane přesouvat vpřed. Poškozený objekt lze identifikovat z FFDC nebo protože se jedná o objekt s nejstarším **MEDIALOG** , když se zobrazí jeho stav v **runmqsc**.

V 9.1.0 Pokud je souborový systém souborů zaplněn a vy se obáváte, že se pracovní zátěž dostane zpět, protože se systém souborů protokolu stává zaplněn, a poté zotavujete objekt, nebo je uvedení do klidového stavu možné zastavit tuto situaci, může dojít k zastavení tohoto procesu.

Zabezpečení souborů protokolu produktu IBM MQ

Nedotýkejte se souborů protokolu, když je správce front spuštěn, obnova může být nemožná. Použijte superuživatele nebo oprávnění mqm k ochraně souborů protokolu proti neúmyslné úpravě.

Neodebírejte aktivní soubory protokolu ručně, je-li spuštěn správce front produktu IBM MQ . Pokud uživatel neúmyslně odstraní soubory protokolu, které správce front potřebuje restartovat, produkt IBM MQ **neprovádí** žádné chyby a pokračuje v zpracování dat *včetně trvalých zpráv*. Správce front se normálně ukončí, ale nespustí se znovu. Navrácení zpráv se pak stane nemožným.

Uživatelé s oprávněním k odebírání protokolů, které jsou používány aktivním správcem front, mají také oprávnění k odstraňování jiných důležitých prostředků správce front (například souborů fronty, katalogu objektů a spustitelných souborů produktu IBM MQ). Mohou tedy poškodit běžící nebo nečinné správce front způsobem, který nedokáže ochránit sám IBM MQ .

Dávejte pozor při udělování superuživatele nebo oprávnění mqm.

Výpis obsahu protokolu pomocí příkazu dmpmqlog

Chcete-li vypsat obsah protokolu správce front, použijte příkaz dmpmqlog .

Chcete-li vypsat obsah protokolu správce front, použijte příkaz dmpmqlog . Standardně jsou všechny aktivní záznamy žurnálu vypsány, to znamená, že příkaz spouští výpis paměti z hlavičky protokolu (obvykle od začátku posledního dokončeného kontrolního bodu).

Protokol lze obvykle vypsat pouze v případě, že není spuštěn správce front. Vzhledem k tomu, že správce front přijímá kontrolní bod během ukončování práce, aktivní část protokolu obvykle obsahuje malý počet záznamů protokolu. Chcete-li však změnit počáteční pozici výpisu paměti, můžete pomocí příkazu dmpmqlog vypsat více záznamů protokolu pomocí jedné z následujících voleb:

- Spuštění výpisu paměti z *báze* protokolu. Základ protokolu je první záznam protokolu v souboru protokolu, který obsahuje hlavičku protokolu. Množství dalších dat vypsaných v tomto případě závisí na tom, kde se hlava protokolu nachází v souboru protokolu. Pokud se blíží ke začátku souboru protokolu, vypíše se pouze malý objem dalších dat. Pokud se hlava nachází v blízkosti konce souboru protokolu, bude vypsána podstatně více dat.

- Určete počáteční pozici výpisu paměti jako jednotlivý záznam protokolu. Každý záznam protokolu je identifikován jedinečným *pořadovým číslem protokolu (LSN)*. V případě kruhového protokolování nesmí tento záznam počátečního protokolu existovat před základní úrovní protokolu; toto omezení se nevztahuje na lineární protokoly. Možná budete muset obnovit neaktivní soubory protokolu před spuštěním příkazu. Je třeba určit platné pořadové číslo v protokolu přijaté z předchozího výstupu příkazu `dmpmqlog` jako počáteční pozici.

  Například s lineárním protokolováním můžete uvést `nextlsn` z posledního výstupu příkazu `dmpmqlog` . Hodnota `nextlsn` se zobrazí v parametru `Log File Header` a udává pořadové číslo v žurnálu dalšího záznamu protokolu, který má být zapsán. Použijte tuto pozici jako počáteční pozici pro formátování všech záznamů protokolu, které byly zapsány od posledního výpisu protokolu.
- **Pouze pro lineární protokoly**můžete instruovat `dmpmqlog` , aby se spustily záznamy protokolu z jakéhokoli daného rozsahu souboru protokolu. V tomto případě příkaz `dmpmqlog` očekává, že tento soubor protokolu najde a každý po sobě jdoucí, ve stejném adresáři jako aktivní soubory protokolu. Tato volba se nevztahuje na kruhové protokoly, kde `dmpmqlog` nemůže získat přístup k záznamům protokolu před založenýmprotokolu.

Výstup z příkazu `dmpmqlog` je `Log File Header` a řada formátovaných záznamů protokolu. Správce front používá několik záznamů žurnálu k zaznamenání změn svých dat.

Některé z informací, které jsou formátovány, se používají pouze interně. Následující seznam obsahuje nejužitečnější záznamy protokolu:

Hlavička souboru žurnálu.
Každý protokol má jediné záhlaví souboru protokolu, což je vždy první věc formátovaná příkazem `dmpmqlog` . Obsahuje následující pole:

logactive = aktivní	Počet oblastí primárního protokolu.
loginactive	Počet sekundárních fyzických oblastí protokolu.
logsize	Počet stránek o velikosti 4 kB za fyzickou oblast.
základsn	První LSN v rozsahu protokolu obsahující hlavu protokolu.
nextlsn	Pořadové číslo LSN dalšího záznamu protokolu, který má být zapsán.
headlsn	Pořadové číslo protokolu záznamu v protokolu v záhlaví protokolu.
tailsn	Pořadové číslo v protokolu LSN označující koncovou pozici protokolu v protokolu.
hflag1	Zda se jedná o protokol CIRCULAR nebo LOG RETAIN (lineární).
HeadExtentID	Oblast protokolu obsahující hlavičku protokolu.

Záhlaví záznamu protokolu
Každý záznam protokolu v rámci protokolu má pevné záhlaví obsahující následující informace:

LSN	Pořadové číslo v protokolu.
LogRecdTyp	Typ záznamu protokolu.
XTrand	Identifikátor transakce přidružený k tomuto záznamu protokolu (pokud existuje). *TranType* rozhraní MQI označuje pouze transakci typu IBM MQ-only. *TranType* z XA se podílí na jiných správcích prostředků. Aktualizace zahrnuté do stejné jednotky práce mají stejný *XTranid*.
QueueName	Fronta přidružená k tomuto záznamu protokolu (pokud existuje).
Qid	Jedinečný vnitřní identifikátor fronty.
PrevLSN	Pořadové číslo předchozího záznamu protokolu v protokolu v rámci stejné transakce (je-li k tomu došlo).

Spustit správce front
Protokoly, které správce front spustil.

StartDate	Datum, kdy byl spuštěn správce front.
StartTime	Čas, kdy byl správce front spuštěn.

Zastavit správce front
Protokoly, které správce front zastavily.

StopDate	Datum, kdy byl zastaven správce front.
StopTime	Čas zastavení správce front.
ForceFlag	Typ použitého ukončení práce.

Začátek kontrolního bodu
To označuje začátek kontrolního bodu správce front.

Koncový kontrolní bod
To označuje konec kontrolního bodu správce front.

ChkPtLSN	Pořadové číslo v protokolu pro záznam protokolu, který spustil tento kontrolní bod.

Vložit zprávu
Tím se protokolují trvalá zpráva do fronty. Pokud byla zpráva vložena pod synchronizační bod, záhlaví záznamu protokolu obsahuje nenull *XTranid*. Zbytek záznamu obsahuje:

MapIndex	Identifikátor pro zprávu ve frontě. Lze ji použít k porovnání odpovídající hodnoty MQGET , která byla použita k získání této zprávy z fronty. V tomto případě může být nalezen následný záznam protokolu *Get Message* obsahující stejné QueueName a MapIndex. V tomto okamžiku lze identifikátor MapIndex znovu použít pro následné vložení zprávy do této fronty.
Data	Obsaženo v hexadecimálním výpisu paměti pro tento záznam protokolu jsou různé vnitřní údaje, následované reprezentací deskriptoru zpráv (eyecatcher MD) a dále samotná data zprávy.

Vložit část
Trvalé zprávy, které jsou příliš velké pro jeden záznam protokolu, se protokolují jako více záznamů protokolu *Put Part* následovaných jediným záznamem *Put Message* . Pokud existují záznamy *Put Part* , pak pole *PrevLSN* bude zřetězit záznamy *Put Part* a konečný záznam *Put Message* dohromady.

Data	Pokračuje v datech zprávy tam, kde byl předchozí záznam protokolu ponechán mimo.

Získat zprávu
Protokolovány jsou pouze přístupy trvalých zpráv. Pokud se zpráva dostala pod synchronizační bod, záhlaví záznamu protokolu obsahuje non-null *XTranid*. Zbytek záznamu obsahuje:

MapIndex	Identifikuje zprávu, která byla načtena z fronty. Nejnovější záznam protokolu *Put Message* obsahující stejné *QueueName* a *MapIndex* identifikuje zprávu, která byla načtena.
Priorita QPriority	Priorita zprávy načtené z fronty.

Spustit transakci
Označuje začátek nové transakce. TranType rozhraní MQI označuje pouze transakci typu IBM MQ. TranType XA označuje název, který zahrnuje další správce prostředků. Všechny aktualizace provedené touto transakcí budou mít stejné *XTranid*.

Připravit transakci
Označuje, že správce front je připraven potvrdit aktualizace přidružené k zadanému *XTranid*. Tento záznam protokolu je zapsán jako součást dvoufázového potvrzování zahrnujícího ostatní správce prostředků.

Potvrdit transakci
Označuje, že správce front provedl potvrzení všech aktualizací provedených transakcí.

Odvolat transakci
To označuje záměr správce front odvolat transakci.

Ukončit transakci
To označuje konec odvolané transakce.

Tabulka transakcí
Tento záznam je zapsán během synchronizačního bodu. Zaznamená stav každé transakce, která provedla trvalé aktualizace. Pro každou transakci jsou zaznamenány následující informace:

XTrand	Identifikátor transakce.
FirstLSN	Pořadové číslo v protokolu prvního záznamu protokolu přidruženého k transakci.
LastLSN	Pořadové číslo v protokolu posledního záznamu protokolu přidruženého k transakci.

Účastníci transakce
Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Záznamy o externích správcích prostředků, kteří se účastní transakcí. Pro každého účastníka se zaznamená následující:

Název RMName	Název správce prostředků.
ID transakce	Identifikátor správce prostředků. To je také zaprotokolováno v následných záznamech protokolu *Transaction Prepared* , které zaznamenávají globální transakce, v nichž se správce prostředků podílí.
SwitchFile	Soubor načtení přepínače pro tohoto správce prostředků.
XAOpenString	Otevřený řetězec XA pro tohoto správce prostředků.
XACloseString	Řetězec zavření XA pro tohoto správce prostředků.

Připravená transakce
Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Označuje, že zadaná globální transakce byla úspěšně připravena. Každý zúčastněný správce prostředků bude instruován k potvrzení. *RMID* každého připraveného správce prostředků je zaznamenáno v záznamu protokolu. Účastní-li se správce front v transakci *Participant Entry* s hodnotou *RMID* , bude přítomna hodnota nula.

Zapomenutí transakce
Tento záznam protokolu je zapsán komponentou správce transakcí XA správce front. Je-li rozhodnutí o potvrzení přijato každému účastníkovi, následuje záznam protokolu produktu *Transaction Prepared* .

Vyprázdnit frontu
Tím se protokolují informace o tom, že všechny zprávy ve frontě byly vyprázdněny, například pomocí příkazu MQSC CLEAR QUEUE.

Atributy fronty
Tím se protokolují inicializace nebo změna atributů fronty.

Vytvořit objekt
Tím se protokolují vytvoření objektu IBM MQ .

ObjName	Název objektu, který byl vytvořen.
UserId	ID uživatele, který provádí vytvoření.

Odstranit objekt
Tím se protokolují odstranění objektu IBM MQ .

ObjName	Název objektu, který byl odstraněn.

Zálohování a obnova dat správce front produktu IBM MQ

Můžete ochránit správce front proti možné korupci způsobené selháním hardwaru tím, že zálohujete správce front a data správce front tak, že zálohujete pouze konfiguraci správce front a použijete záložní správce front.

Informace o této úloze

POZOR: Pokud přesouváte správce front do jiného operačního systému, je třeba se velmi pečlivě starat o jeho přesunutí. Další informace najdete v tématu Přesun správce front na jiný operační systém .

Periodicky můžete přijmout opatření k ochraně správců front proti možnému poškození způsobenému hardwarovými poruchami. Existují tři způsoby ochrany správce front:

Zálohovat data správce front
Dojde-li k selhání hardwaru, může být vynucen jeho zastavení správce front. Dojde-li ke ztrátě dat protokolu správce front v důsledku selhání hardwaru, může být správce front schopen restartovat. Pokud zálohujete data správce front, můžete být schopni obnovit některé nebo všechny údaje o ztracených datech správce front.

Obecně platí, že čím častěji zálohujete data správce front, tím méně dat ztratíte v případě selhání hardwaru, které vede ke ztrátě integrity protokolu pro zotavení.

Chcete-li zálohovat data správce front, nesmí být správce front spuštěn.

Zálohovat pouze konfiguraci správce front
Dojde-li k selhání hardwaru, může být vynucen jeho zastavení správce front. Dojde-li ke ztrátě konfigurace správce front i dat protokolu v důsledku selhání hardwaru, nebude se správce front moci restartovat nebo jej lze z protokolu obnovit. 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 správce front zálohování
Je-li selhání hardwaru závažné, může být správce front nezotavitelný. V této situaci může být správce front zálohy aktivován v případě neodstranitelného správce front, pokud má správce front nezotavitelné správce front vyhrazené záložní správce front. Je-li záznam aktualizován pravidelně, může protokol správce front zálohy obsahovat data protokolu, která obsahují poslední dokončený protokol ze nezotavitelného správce front.

Záložní správce front může být aktualizován v době, kdy je stále spuštěn existující správce front.

Procedura

- Chcete-li zálohovat a obnovit data správce front, prohlédněte si:
  - “Zálohování dat správce front” na stránce 602.
  - “Obnova dat správce front” na stránce 603.
- Chcete-li zálohovat a obnovit konfiguraci správce front, přečtěte si následující informace:

  - “Zálohování konfigurace správce front” na stránce 603
  - “Obnovení konfigurace správce front” na stránce 604
- Chcete-li vytvořit, aktualizovat a spustit správce front zálohování, prohlédněte si téma “Použití správce front zálohování” na stránce 605.

Zálohování dat správce front

Zálohování dat správce front vám může pomoci chránit před možnou ztrátou dat způsobenou hardwarovými chybami.

Než začnete

Před zahájením zálohování správce front se ujistěte, že správce front není spuštěn. Pokud se pokusíte provést zálohu spuštěného správce front, záloha nemusí být konzistentní, protože při kopírování souborů dojde k jeho aktualizacím. Je-li to možné, zastavte správce front spuštěním příkazu **endmqm -w** (čekání na ukončení práce systému), pouze pokud k tomu dojde, použijte příkaz **endmqm -i** (okamžité ukončení činnosti).

Informace o této úloze

Chcete-li vytvořit záložní kopii dat správce front, proveďte následující úlohy:

Postup

1. Vyhledejte adresáře, pod kterými správce front umisťuje svá data a soubory protokolu za použití informací v konfiguračních souborech.

   Další informace viz téma “Změna informací o konfiguraci IBM MQ v souborech .ini na platformě Multiplatforms” na stránce 81.

   Poznámka: Názvy, které se v adresáři objeví, se transformují, aby se zajistilo, že jsou kompatibilní s platformou, na které používáte produkt IBM MQ. Další informace o transformacích názvů najdete v tématu Základní informace o názvech souborů produktu IBM MQ.
2. Převeďte kopie všech dat správce front a adresářů souborů protokolu, včetně všech podadresářů.

   Ujistěte se, že nechybí žádné soubory, zejména řídicí soubor protokolu, jak je popsáno v části “Jaké protokoly vypadají jako” na stránce 573, a konfigurační soubory, jak je popsáno v tématu “Inicializační a konfigurační soubory” na stránce 216. Některé adresáře mohou být prázdné, ale vy je budete potřebovat k obnovení zálohy později.

   Pro kruhové protokolování zálohujte data správce front a adresáře souborů protokolu ve stejnou dobu, abyste mohli obnovit konzistentní sadu dat a protokolů správce front.

   V případě lineární protokolování zálohujte data správce front a adresáře souborů protokolu současně. Je-li k dispozici odpovídající úplná posloupnost souborů žurnálu, je možné obnovit pouze datové soubory správce front.
3. Zachovejte vlastnictví souborů.

   Linux UNIX Pro systémy IBM MQ for UNIX a Linux to můžete provést pomocí příkazu **tar** . (Máte-li fronty větší než 2 GB, nelze použít příkaz **tar** . Další informace naleznete v tématu Povolení velkých front.

   Poznámka: Provedete-li upgrade na produkt IBM WebSphere MQ 7.5 a později, ujistěte se, že jste provedli zálohu souboru `qm.ini` a položek registru. Informace o správci front jsou uloženy v souboru `qm.ini` a lze je použít k vrácení zpět na předchozí verzi produktu IBM MQ.

Související úlohy

Zastavení správce front

“Zálohování konfiguračních souborů po vytvoření správce front” na stránce 14

Konfigurační informace produktu IBM MQ jsou uloženy v konfiguračních souborech v systému UNIX, Linux, and Windows. Po vytvoření správce front zazálohujte své konfigurační soubory. Pokud pak vytvoříte

jiného správce front, který způsobuje problémy, můžete zálohy obnovit, až odeberete zdroj daného problému.

Obnova dat správce front

Chcete-li obnovit zálohu dat správce front, postupujte podle následujících kroků.

Než začnete

Před spuštěním zálohy se ujistěte, že správce front není spuštěn.

Když obnovujete zálohu správce front v klastru, prohlédněte si téma “Obnova správce front klastru” na stránce 341 a Klastrování: Availability, multi-instance a disaster recovery , kde získáte další informace.

Poznámka: Když provádíte upgrade na novější verzi produktu IBM MQ, ujistěte se, že jste provedli zálohu souboru **.ini** a položek registru. Informace o správci front jsou uloženy v souboru **.ini** a lze je použít k vrácení zpět na předchozí verzi produktu IBM MQ.

Postup

1. Pomocí informací v konfiguračních souborech vyhledejte adresáře, pod kterými správce front umisťuje svá data a příslušné soubory protokolu.
2. Vyprázdněte adresáře, do kterých chcete umístit data typu "backedup".
3. Zkopírujte data správce front-up a soubory protokolu do správných míst.

   Ujistěte se, že máte soubor s řízením protokolu a také soubory protokolu.

   Pro kruhové protokolování zálohujte data správce front a adresáře souborů protokolu ve stejnou dobu, abyste mohli obnovit konzistentní sadu dat a protokolů správce front.

   V případě lineární protokolování zálohujte data správce front a adresáře souborů protokolu současně. Je-li k dispozici odpovídající úplná posloupnost souborů žurnálu, je možné obnovit pouze datové soubory správce front.
4. Aktualizujte soubory s informacemi o konfiguraci.

   Zkontrolujte, zda jsou konfigurační soubory IBM MQ a správce front konzistentní, takže produkt IBM MQ může vyhledávat obnovená data na správných místech.
5. Zkontrolujte výslednou adresářovou strukturu a ujistěte se, že máte všechny požadované adresáře.

   Další informace o adresářích a podadresářích produktu IBM MQ viz Adresářová struktura v systémech Windows a Obsah adresáře v systémech UNIX and Linux.

Výsledky

Pokud byla data zálohována a obnovena správně, bude správce front nyní spuštěn.

Multi Zálohování konfigurace správce front

Zálohování konfigurace správce front vám může pomoci znovu sestavit správce front z definic, pokud dojde ke ztrátě konfigurace správce front i dat protokolu kvůli selhání hardwaru, a správce front se nemůže restartovat nebo aby byl obnoven z protokolu.

Informace o této úloze

ULW V systému UNIX, Linux, and Windowsmůžete pomocí příkazu **dmpmqcfg** vypsat konfiguraci správce front IBM MQ .

IBM i V systému IBM imůžete použít příkaz Výpis paměti MQ (**DMPMQMCFG**) k výpisu konfiguračních objektů a oprávnění správce front.

Postup

1. Ověřte, že je spuštěn správce fronty.
2. V závislosti na použité platformě použijte jeden z následujících příkazů k zálohování konfigurace správce front:
   - ULW V systému UNIX, Linux, and Windows: Provést příkaz konfigurace výpisu paměti MQ , **dmpmqcfg**pomocí výchozí volby formátování (-f mqsc) MQSC a všech atributů (-a), použijte přesměrování standardního výstupu pro ukládání definic do souboru. Příklad:

     ```
     dmpmqcfg -m MYQMGR -a > /mq/backups/MYQMGR.mqsc
     ```

   - IBM i V systému IBM i: Provést příkaz výpisu paměti MQ (**DMPMQMCFG**) s použitím výchozí volby formátování OUTPUT (*MQSC) a EXPATTR (*ALL), použijte soubory 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 604
Můžete obnovit konfiguraci správce front ze zálohy tak, že nejprve ověřte, zda je správce front spuštěn, a poté spusťte příslušný příkaz pro příslušnou platformu.

Související odkazy

dmpmqcfg (konfigurace správce front výpisu)
Výpis konfigurace MQ (DMPMQMCFG)

Multi Obnovení konfigurace správce front

Můžete obnovit konfiguraci správce front ze zálohy tak, že nejprve ověřte, zda je správce front spuštěn, a poté spusťte příslušný příkaz pro příslušnou platformu.

Informace o této úloze

ULW V systému UNIX, Linux, and Windowsmůžete použít příkaz **runmqsc** k obnovení konfigurace správce front IBM MQ .

IBM i V systému IBM imůžete pomocí příkazu **STRMQMMQSC** obnovit konfigurační objekty a oprávnění pro správce front.

Postup

1. Ověřte, že je spuštěn správce fronty.

   Všimněte si, že pokud je poškození dat a protokolů neopravitelné jiným způsobem, mohl by být správce front znovu vytvořen.
2. V závislosti na použité platformě použijte jeden z následujících příkazů k obnově konfigurace správce front:
   - ULW V systému UNIX, Linux, and Windowsspusťte **runmqsc** proti správci front, použijte přesměrování standardního vstupu pro obnovení definic ze skriptového souboru generovaného příkazem MQ Dump (**dmpmqcfg**) (viz “Zálohování konfigurace správce front” na stránce 603). Příklad:

     ```
     runmqsc MYQMGR < /mq/backups/MYQMGR.mqsc
     ```

- IBM i V systému IBM i: Spusťte **STRMQMMQSC** proti správci front a pomocí parametrů **SRCMBR** a **SRCFILE** obnovte definice z členu fyzického souboru generovaný příkazem Výpis paměti MQ (**DMPMQMCFG**) (viz “Zálohování konfigurace správce front” na stránce 603). Příklad:

```
STRMQMMQSC MQMNAME(MYQMGR) SRCFILE(QMQMSAMP/QMQSC) SRCMBR(MYQMGR)
```

Související úlohy

“Zálohování konfigurace správce front” na stránce 603
Zálohování konfigurace správce front vám může pomoci znovu sestavit správce front z definic, pokud dojde ke ztrátě konfigurace správce front i dat protokolu kvůli selhání hardwaru, a správce front se nemůže restartovat nebo aby byl obnoven z protokolu.

Související odkazy

dmpmqcfg (konfigurace správce front výpisu)
runmqsc (spuštění příkazů MQSC)
Výpis konfigurace MQ (DMPMQMCFG)
Spuštění příkazů IBM MQ (STRMQMMQSC)

Použití správce front zálohování

Existující správce front může mít pro účely zotavení z havárie vyhrazený správce front pro zotavení z havárie.

Informace o této úloze

Záložní správce front je neaktivní kopie existujícího správce front. Pokud se stávající správce front stane neobnovitelným kvůli závažnému selhání hardwaru, lze správce front zálohy převést do režimu online a nahradit neodstranitelného správce front.

Existující soubory protokolu správce front musí být pravidelně kopírovány do správce front zálohování, aby bylo zajištěno, že správce front zálohování zůstane účinnou metodou pro zotavení z havárie. The existing queue manager does not need to be stopped for log files to be copied, however you should only copy a log file if the queue manager has finished writing to it; see “Aktualizace záložního správce front” na stránce 606 for information on how to ensure a specific log file is not being written to anymore, so that it can be safely copied.

Poznámka: Protože se existující protokol správce front průběžně aktualizuje, je mezi stávajícím protokolem správce front a daty protokolu zkopírovanými do protokolu správce front pro zálohování zkopírováno nepatrné rozdíly mezi existujícím protokolem správce front a daty protokolu. Pravidelné aktualizace správce front zálohování minimalizuje rozdíly mezi dvěma protokoly.

Je-li nutné správce front zálohování převést do režimu online, musí být aktivován a poté spuštěn. Požadavek na aktivaci správce front zálohy předtím, než je spuštěn, je preventivní opatření, které má být chráněno proti náhodnému spuštění zálohovacího správce front. Poté, co je správce front zálohování aktivován, již jej nelze aktualizovat.

Důležité: Jakmile se starý záložní správce front stane novým aktivním správcem front, z libovolného důvodu již neexistuje správce front zálohování. Toto je efektivní forma asynchronní replikace, a proto se očekává, že nový aktivní správce front bude logicky nějaký čas za starým aktivním správcem front. Jako takový se starý aktivní správce front již nebude chovat jako záloha pro nového aktivního správce front.

Procedura

- Informace o použití správce front zálohy naleznete v následujících tématech:
  - “Vytvoření správce front zálohování” na stránce 606
  - “Aktualizace záložního správce front” na stránce 606
  - “Spuštění záložního správce front” na stránce 607

Související pojmy

“Protokolování: Ujištění se, že zprávy nejsou ztraceny” na stránce 573

Příkaz IBM MQ zaznamenává všechny významné změny trvalých dat řízených správcem front v protokolu pro zotavení.

Vytvoření správce front zálohování

Záložní správce front vytvoříte jako neaktivní kopii existujícího správce front.

Informace o této úloze

Důležité: Při použití lineárního protokolování můžete použít pouze správce front zálohování.

Záložní správce front vyžaduje následující:

- Chcete-li mít stejné atributy jako existující správce front, například název správce front, typ protokolování a velikost souboru protokolu.
- Má být na stejné platformě jako existující správce front.
- Být na stejné nebo vyšší úrovni kódu, než je úroveň kódu existující správce front.

Postup

1. Vytvořte správce front zálohy pro existujícího správce front pomocí příkazu ovládacího prvku **crtmqm**.
2. Převeďte kopie všech existujících dat správce front a adresářů souborů protokolu, včetně všech podadresářů, jak je popsáno v tématu “Zálohování dat správce front” na stránce 602.
3. Přepište soubory dat a adresáře souborů správce front zálohování, včetně všech podadresářů, s kopiemi převzatovanými z existujícího správce front.
4. Spusťte řídicí příkaz **strmqm** na správci front zálohy, jak je uvedeno v následujícím příkladu:

   ```
   strmqm -r BackupQMName
   ```

   Tento příkaz označí správce front jako správce front zálohy v rámci produktu IBM MQa přehraje všechny zkopírované oblasti protokolu k převedení správce front zálohy v kroku s existujícím správcem front.

Související odkazy

crtmqm (vytvoření správce front)

strmqm (spuštění správce front)

Aktualizace záložního správce front

Chcete-li zajistit, aby záložní správce front zůstal účinnou metodou pro zotavení z havárie, musí být pravidelně aktualizován.

Informace o této úloze

Pravidelná aktualizace snižuje rozdíly mezi záložním protokolem správce front protokolu a aktuálním protokolem správce front. Před tím, než budete zálohovat, není třeba správce front zastavit.

Upozornění: Pokud kopírujete nesouvislou sadu protokolů do adresáře protokolu správce front zálohy, bude přehrán pouze protokol až do místa, kde je nalezen první chybějící protokol.

Postup

1. Na správce front, který má být zálohován, zadejte následující příkaz skriptu (MQSC):

   ```
   RESET QMGR TYPE(ADVANCELOG)
   ```

   Tím dojde k zastavení libovolného zápisu do aktuálního protokolu a následné zálohy protokolování správce front do dalšího rozsahu protokolu. Tím je zajištěno, že zálohujete všechny informace zaprotokolované do aktuálního času.

2. Získejte (nové) aktuální číslo fyzické oblasti aktivního protokolu zadáním následujícího příkazu skriptu (MQSC) na správci front, který má být zálohován:

```
DIS QMSTATUS CURRLOG
```

3. Zkopírujte aktualizované soubory oblastí protokolu z aktuálního adresáře protokolu správce front do adresáře protokolu správce front zálohy.

   Zkopírujte všechny fyzické oblasti protokolu od poslední aktualizace a do (ale ne včetně) aktuální fyzické oblasti uvedené v “2” na stránce 607. Kopírovat pouze soubory rozsahu protokolu, ty začínající znaky "S. ..".

4. Spusťte řídicí příkaz **strmqm** na správci front zálohy, jak je uvedeno v následujícím příkladu:

   ```
   strmqm -r BackupQMName
   ```

   Tím přehraje všechny kopírované oblasti protokolu a převede správce front do kroku se správcem front. Jakmile se přehrávání dokončí, obdržíte zprávu, která identifikuje všechny oblasti, které jsou nezbytné pro obnovu restartu, a všechny oblasti, které jsou nezbytné pro obnovení médií.

Související odkazy
RESETOVAT QMGR
ZOBRAZIT STAV QM
strmqm (spuštění správce front)

Spuštění záložního správce front

Záložní správce front můžete nahradit nezotavitelným správcem front.

Informace o této úloze

Když obnovujete zálohu správce front v klastru, prohlédněte si téma “Obnova správce front klastru” na stránce 341 a Klastrování: Availability, multi-instance a disaster recovery , kde získáte další informace.

Pokud má nezotavitelný správce front vyhrazený správce front zálohování, můžete správce front zálohování aktivovat na místě neodstranitelného správce front.

Když je správce front zálohování nahrazen nezotavitelným správcem front, mohou být některé údaje správce front ze správce front nezotavitelného správce ztraceny. Množství ztracených dat závisí na tom, jak nedávno byl správce front zálohování naposledy aktualizován. Čím novější je poslední aktualizace, tím menší ztráta dat správce front.

Poznámka: I když jsou data správce front a soubory protokolu uloženy v různých adresářích, ujistěte se, že zálohujete a obnovujete adresáře ve stejnou dobu. Pokud se data a soubory protokolu správce front liší od stáří, správce front se nenachází v platném stavu a pravděpodobně nebude spuštěn. I když se to spustí, vaše data pravděpodobně budou poškozená.

Postup

1. Spuštěním řídicího příkazu **strmqm** aktivujte správce front zálohy tak, jak je uvedeno v následujícím příkladu:

   ```
   strmqm -a BackupQMName
   ```

   Záložní správce front je aktivován. Nyní, když je aktivní, záložní správce front již nebude moci být aktualizován.

2. Spuštěním řídicího příkazu **strmqm** spusťte správce front zálohy, jak je uvedeno v následujícím příkladu:

   ```
   strmqm BackupQMName
   ```

IBM MQ považuje toto zotavení za opětné spuštění a používá protokol ze správce front zálohování. Během poslední aktualizace pro správce front zálohování se vyskytne přehrání, proto se odvolají pouze aktivní transakce z naposledy zaznamenaného kontrolního bodu.

3. Restartujte všechny kanály.
4. Zkontrolujte výslednou adresářovou strukturu a ujistěte se, že máte všechny požadované adresáře.

   Další informace o adresářích a podadresářích aplikačního serveru IBM MQ najdete v tématu Plánování podpory systému souborů.
5. Ujistěte se, že máte soubor s řízením protokolu a také soubory protokolu. Také zkontrolujte, zda jsou konfigurační soubory produktu IBM MQ a správce front konzistentní, aby se produkt IBM MQ mohl podívat na správná místa obnovených dat.

Výsledky

Pokud byla data zálohována a obnovena správně, bude nyní spuštěn správce front.

Související úlohy

“Restartování zastavených kanálů” na stránce 210
Když kanál přejde do stavu STOPPED, je nutné kanál restartovat ručně.

Související odkazy

strmqm (spuštění správce front)

Změny v zotavení z chyb klastru (na serverech jiných než z/OS)

Počínaje produktem IBM WebSphere MQ 7.1 správce front znovu spouští operace, které způsobily problémy, dokud nejsou problémy vyřešeny. Pokud po uplynutí pěti dnů nebudou problémy vyřešeny, správce front se ukončí, aby zabránil tomu, aby se mezipaměť nestala aktuální.

Před IBM WebSphere MQ 7.1, pokud správce front zjistil problém s lokálním správcem úložiště spravujícím klastr, aktualizoval protokol chyb. V některých případech pak zastavil správu klastrů. Správce front nadále vyměňuje zprávy aplikací s klastrem a spoléhá se na jejich stále více neaktuální mezipaměti definic klastru. Počínaje produktem IBM WebSphere MQ 7.1 správce front znovu spouští operace, které způsobily problémy, dokud nejsou problémy vyřešeny. Pokud po uplynutí pěti dnů nebudou problémy vyřešeny, správce front se ukončí, aby zabránil tomu, aby se mezipaměť nestala aktuální. Protože je mezipaměť stále více zastaralá, způsobuje větší počet problémů. Změněné chování týkající se chyb klastru ve verzi 7.1 nebo pozdější se nevztahuje na z/OS.

Každý aspekt správy klastru je zpracováván pro správce front procesem správce lokálního úložiště, `amqrrmfa`. Proces se spustí ve všech správcích front, a to i v případě, že neexistují žádné definice klastrů.

Před IBM WebSphere MQ 7.1, pokud správce front zjistil problém v lokálním správci úložiště, zastavil správce úložiště po krátkém intervalu. Správce front byl stále spuštěn, zpracovává zprávy aplikací a požadavky na otevřené fronty a publikoval nebo odebíráte témata.

Po zastavení správce úložiště se mezipaměť definic klastru, která je k dispozici správci front, stala zastaralejší. V průběhu času byly zprávy směrovány do špatného místa určení a aplikace se nezdařily. Aplikace se nezdařily při pokusu o otevření front klastru nebo témat publikování, která nebyla šířena do lokálního správce front.

Pokud administrátor nezakontroloval zprávy úložiště v protokolu chyb, administrátor možná neuvědomuje, že konfigurace klastru má problémy. Pokud nebylo selhání rozpoznáno za delší dobu a správce front neobnovil své členství v klastru, došlo k ještě většímu počtu problémů. Nestabilita ovlivnila všechny správce front v klastru a klastr se ukázal jako nestabilní.

Počínaje produktem IBM WebSphere MQ 7.1 používá produkt IBM MQ odlišný přístup ke zpracování chyb klastru. Místo zastavení správce úložiště a jeho ponechání bez něj znovu selhávají operace správce úložiště. Pokud správce front zjistí problém se správcem úložiště, bude postupovat podle jednoho ze dvou cyklů akce.

1. Pokud chyba neohrožuje činnost správce front, zapíše zprávu do protokolu chyb zprávu správce front. Oběhne selhané operace každých 10 minut, dokud nebude operace úspěšná. Ve výchozím nastavení

máte pět dní na vyřešení chyby; v opačném případě správce front zapíše zprávu do protokolu chyb a ukončí se. Můžete odložit o pět dnů vypnutí.

2. Pokud chyba ohrožuje činnost správce front, zapíše zprávu do protokolu chyb zprávu a ihned ukončí práci.

Chyba, která ohrožuje činnost správce front, je chyba, kterou správce front nemohl diagnostikovat, nebo chybu, která může mít nepředvídatelné následky. Tento typ chyby často vede k tomu, že správce front zapisuje soubor FFST . Chyby, které narušují činnost správce front, může být způsobeno chybou v produktu IBM MQnebo administrátorem nebo programem, který provádí něco neočekávaného, jako např. ukončení procesu IBM MQ .

Cílem změny v chování při zotavení z chyb je omezit dobu spuštění správce front s rostoucím počtem nekonzistentních definic klastru. Vzhledem k tomu, že počet nekonzistencí v definicích klastrů roste, s tím roste i pravděpodobnost nestandardního chování aplikací.

Výchozí volbou vypnutí správce front po pěti dnech je kompromis mezi omezením počtu nekonzistencí a udržováním dostupnosti správce front, dokud nejsou zjištěny a vyřešeny problémy.

Můžete prodloužit dobu, než se správce front ukončí neomezeně dlouho, zatímco problém opravíte, nebo počkejte na plánované ukončení práce správce front. Hodnota pětidenního pobytu uchovává správce front dlouhým víkendem, což vám dává čas reagovat na případné problémy nebo prodlužovat dobu před restartováním správce front.

Opravné akce

Máte možnost výběru akcí pro řešení problémů s obnovou chyb klastru. První možností je monitorovat a opravit problém, druhý pro monitorování a odložení odstranění problému a poslední možnost je pokračovat ve správě zotavení z chyb klastru jako ve vydáních před produktem IBM WebSphere MQ 7.1.

1. Sledujte protokol chyb správce front a vyhledejte chybové zprávy AMQ9448 a AMQ5008a odstraňte problém.

   AMQ9448 označuje, že správce úložiště vrátil chybu po spuštění příkazu. Tato chyba označuje spuštění příkazu znovu každých 10 minut a nakonec se správce front zastaví po uplynutí pěti dnů, pokud neodložíte ukončení činnosti systému.
   AMQ5008 označuje, že správce front byl zastaven, protože chybí proces IBM MQ . AMQ5008 má za následek zastavení činnosti správce úložiště po pěti dnech. Pokud se správce úložiště zastaví, zastaví se správce front.

2. Sledujte protokol chyb správce front a vyhledejte chybovou zprávu AMQ9448a odložte opravu problému.

   Pokud zakážete načítání zpráv z produktu `SYSTEM.CLUSTER.COMMAND.QUEUE`, správce úložišť se zastaví při pokusu o spuštění příkazů a pokračuje neomezeně bez zpracování jakékoli práce. Uvolní se však všechny obslužné rutiny, které správce úložiště drží ve frontách. Vzhledem k tomu, že se správce úložiště nezastaví, správce front se po pěti dnech nezastaví.
   Spusťte příkaz MQSC pro zakázání 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)
   ```

3. Vraťte správce front na stejné chování při zotavení z chyb klastru jako před IBM WebSphere MQ 7.1.

   Chcete-li správce front v případě zastavení správce úložiště zastavit, můžete nastavit parametr ladění správce front.
   Parametr ladění je `TolerateRepositoryFailure`, ve stanze `TuningParameters` souboru `qm.ini` . Chcete-li zabránit zastavení správce front v případě, že se správce úložiště zastaví, nastavte parametr `TolerateRepositoryFailure` na hodnotu TRUE, viz Obrázek 88 na stránce 610.
   Restartujte správce front, abyste povolili volbu `TolerateRepositoryFailure` .

Pokud došlo k chybě klastru, která brání úspěšnému spuštění správce úložiště, a tím od spuštění správce front, nastavte produkt `TolerateRepositoryFailure` na hodnotu TRUE , aby správce front spustil bez správce úložiště.

Zvláštní pozornost

Před IBM WebSphere MQ 7.1někteří administrátoři spravující správce front, kteří nebyli součástí klastru, zastavili proces `amqrrmfa` . Zastavení `amqrrmfa` neovlivnilo správce front.

Zastavení produktu `amqrrmfa` v produktu IBM WebSphere MQ 7.1 nebo pozdější způsobí zastavení správce front, protože je považován za selhání správce front. Pokud nenastavíte parametr ladění správce front `TolerateRepositoryFailure`, nesmíte zastavit proces produktu `amqrrmfa` ve verzi 7.1 nebo pozdější.

Příklad

```
TuningParameters:
        TolerateRepositoryFailure=TRUE
```

Obrázek 88. Nastavte `TolerateRepositoryFailure` na TRUE v souboru qm.ini

Související pojmy

Konfigurační soubory správce front qm.ini

Konfigurace prostředků produktu JMS

Jedním z způsobů, jak může aplikace produktu JMS vytvořit a konfigurovat prostředky, které potřebuje pro připojení k produktu IBM MQ a k místům určení pro odesílání nebo příjem zpráv, je pomocí rozhraní JNDI (Java Naming and Directory Interface) načítat spravované objekty z umístění v rámci služby pro správu pojmenování a adresářů, která se nazývá obor názvů JNDI. Než bude moci aplikace JMS načíst spravované objekty z oboru názvů JNDI, musíte nejprve vytvořit a nakonfigurovat spravované objekty.

Informace o této úloze

Spravované objekty v produktu IBM MQ můžete vytvářet a konfigurovat pomocí jednoho z následujících nástrojů:

IBM MQ Explorer
Pomocí produktu IBM MQ Explorer můžete vytvářet a spravovat definice objektů produktu JMS , které jsou uloženy v LDAP, v lokálním systému souborů nebo v jiných umístěních.

Administrační nástroj produktu IBM MQ JMS
Administrativní nástroj produktu IBM MQ JMS je nástroj příkazového řádku, který můžete použít k vytvoření a konfiguraci objektů produktu IBM MQ JMS uložených v LDAP, v lokálním systému souborů nebo v jiných umístěních. Administrativní nástroj produktu JMS používá syntaxi podobnou produktu **runmqsc**a také podporuje skriptování.

Nástroj pro správu používá konfigurační soubor k nastavení hodnot určitých vlastností. K dispozici je ukázkový konfigurační soubor, který můžete upravit tak, aby vyhovoval vašemu systému, než začnete používat nástroj ke konfiguraci prostředků produktu JMS . Další informace o konfiguračním souboru viz téma “Konfigurace nástroje pro administraci produktu JMS” na stránce 617.

Aplikace produktu IBM MQ JMS , které jsou implementovány do produktu WebSphere Application Server , potřebují přistupovat k objektům produktu JMS z úložiště JNDI aplikačního serveru. Proto pokud používáte systém zpráv produktu JMS mezi WebSphere Application Server a IBM MQ, musíte vytvořit objekty v WebSphere Application Server , které odpovídají objektům, které vytvoříte v produktu IBM MQ.

IBM MQ Explorer a administrační nástroj produktu IBM MQ JMS nelze použít ke správě objektů produktu IBM MQ JMS uložených v produktu WebSphere Application Server. Místo toho můžete

vytvořit a konfigurovat spravované objekty v produktu WebSphere Application Server pomocí jednoho z následujících nástrojů:

WebSphere Application Server Administrativní konzola
Administrativní konzola produktu WebSphere Application Server je webový nástroj, který lze použít ke správě objektů produktu IBM MQ JMS v produktu WebSphere Application Server.

WebSphere Application Server skriptovací klient wsadmin
Skriptovací klient wsadmin produktu WebSphere Application Server poskytuje specializované příkazy pro správu objektů produktu IBM MQ JMS v produktu WebSphere Application Server.

Chcete-li použít aplikaci JMS pro přístup k prostředkům správce front produktu IBM MQ z produktu WebSphere Application Server, musíte použít poskytovatele systému zpráv produktu IBM MQ v produktu WebSphere Application Server, který obsahuje verzi produktu IBM MQ classes for JMS. Adaptér prostředků produktu IBM MQ , který je dodáván s produktem WebSphere Application Server , používají všechny aplikace, které provozují systém zpráv produktu JMS s poskytovatelem systému zpráv produktu IBM MQ . Adaptér prostředku produktu IBM MQ se obvykle aktualizuje automaticky při použití opravných sad WebSphere Application Server , ale pokud jste již dříve ručně aktualizovali adaptér prostředků, musíte ručně aktualizovat konfiguraci, abyste se ujistili, že je údržba správně aplikována.

Související úlohy
Zápis aplikací IBM MQ classes for JMS
Související odkazy
runmqsc

Konfigurace továren připojení a míst určení v oboru názvů JNDI

Aplikace produktu JMS přistupují ke spravovaným objektům v rámci služby pro správu pojmenování a adresářů prostřednictvím rozhraní JNDI (Java Naming and Directory Interface). Spravované objekty produktu JMS jsou uloženy v umístění v rámci služby pro správu pojmenování a adresářů, na které se odkazuje jako na obor názvů JNDI. Aplikace JMS může vyhledat spravované objekty a připojit se k IBM MQ a přistupovat k místům určení pro odesílání nebo příjem zpráv.

Informace o této úloze

Aplikace produktu JMS vyhledají názvy objektů produktu JMS ve službě pro správu pojmenování a adresářů s použitím kontextů:

počáteční kontext
Počáteční kontext definuje kořen oboru názvů JNDI. Pro každé umístění ve službě pro správu pojmenování a adresářů musíte zadat počáteční kontext, ze kterého uvedete počáteční bod, ze kterého může aplikace JMS vyřešit názvy spravovaných objektů v tomto umístění služby pro pojmenování a adresářovou službu.

Dílčí kontexty
Kontext může mít jeden nebo více dílčích kontextů. Dílčí kontext je dílčím oddílem oboru názvů JNDI a může obsahovat spravované objekty, jako jsou továrny připojení a místa určení, stejně jako další dílčí kontexty. Dílčí kontext není sám o sobě objektem. Je pouze rozšířením konvence pojmenování objektů v dílčím kontextu.

Kontexty můžete vytvořit buď pomocí produktu IBM MQ Explorer , nebo pomocí nástroje pro administraci produktu IBM MQ JMS .

Než bude moci aplikace IBM MQ classes for JMS načíst spravované objekty z oboru názvů JNDI, musíte nejprve vytvořit spravované objekty buď pomocí produktu IBM MQ Explorer , nebo pomocí nástroje pro administraci produktu IBM MQ JMS . Můžete vytvářet a konfigurovat následující typy objektů produktu JMS :

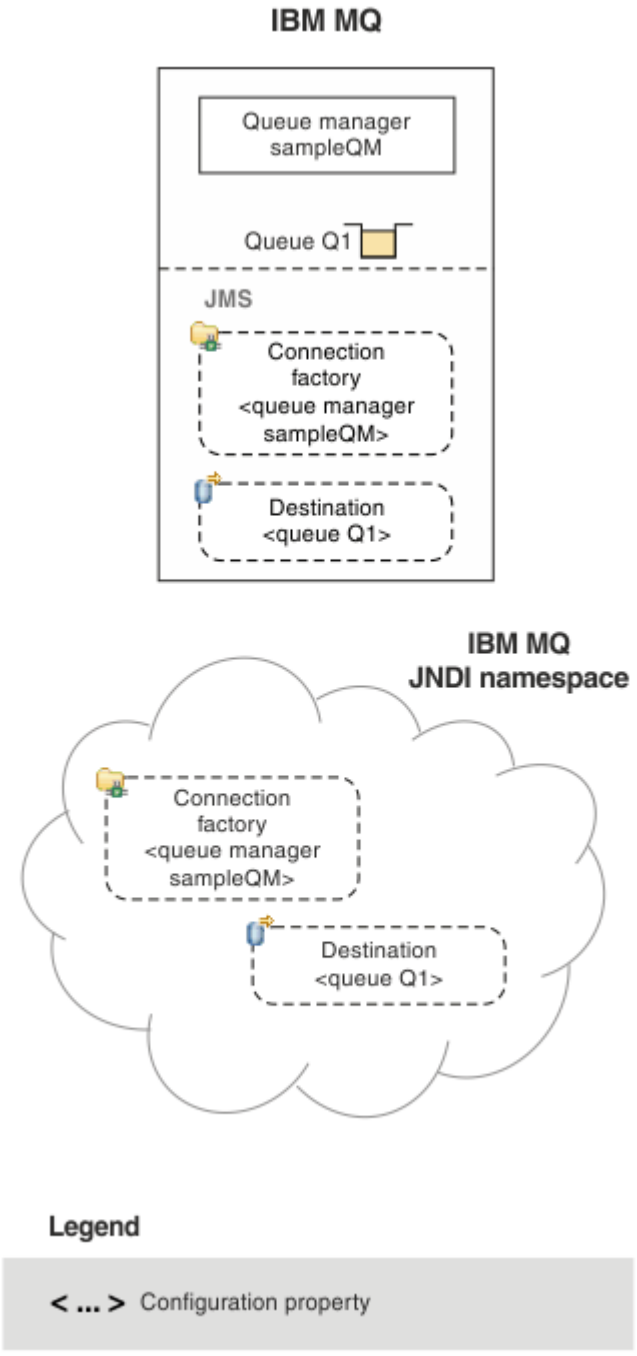
Továrna připojení
Objekt faktorie připojení produktu JMS definuje sadu standardních vlastností konfigurace pro připojení. Aplikace JMS používá továrnu připojení k vytvoření připojení k produktu IBM MQ. Můžete vytvořit továrnu připojení, která je specifická pro jednu z těchto domén systému zpráv, doménu

systému zpráv typu point-to-point a doménu systému zpráv publikování/odběru. Volitelně můžete z produktu JMS 1.1vytvořit továrny připojení nezávislé na doméně, které lze použít pro systém zpráv typu point-to-point i publikování/odběr.

Místo určení
Místo určení JMS je objekt, který představuje cíl zpráv, které klient produkuje, a zdroj zpráv, které aplikace JMS přijímá. Aplikace JMS může buď použít jediný cílový objekt pro vkládání zpráv a získání zpráv od nich, nebo může aplikace používat samostatné cílové objekty. Existují dva typy cílového objektu:

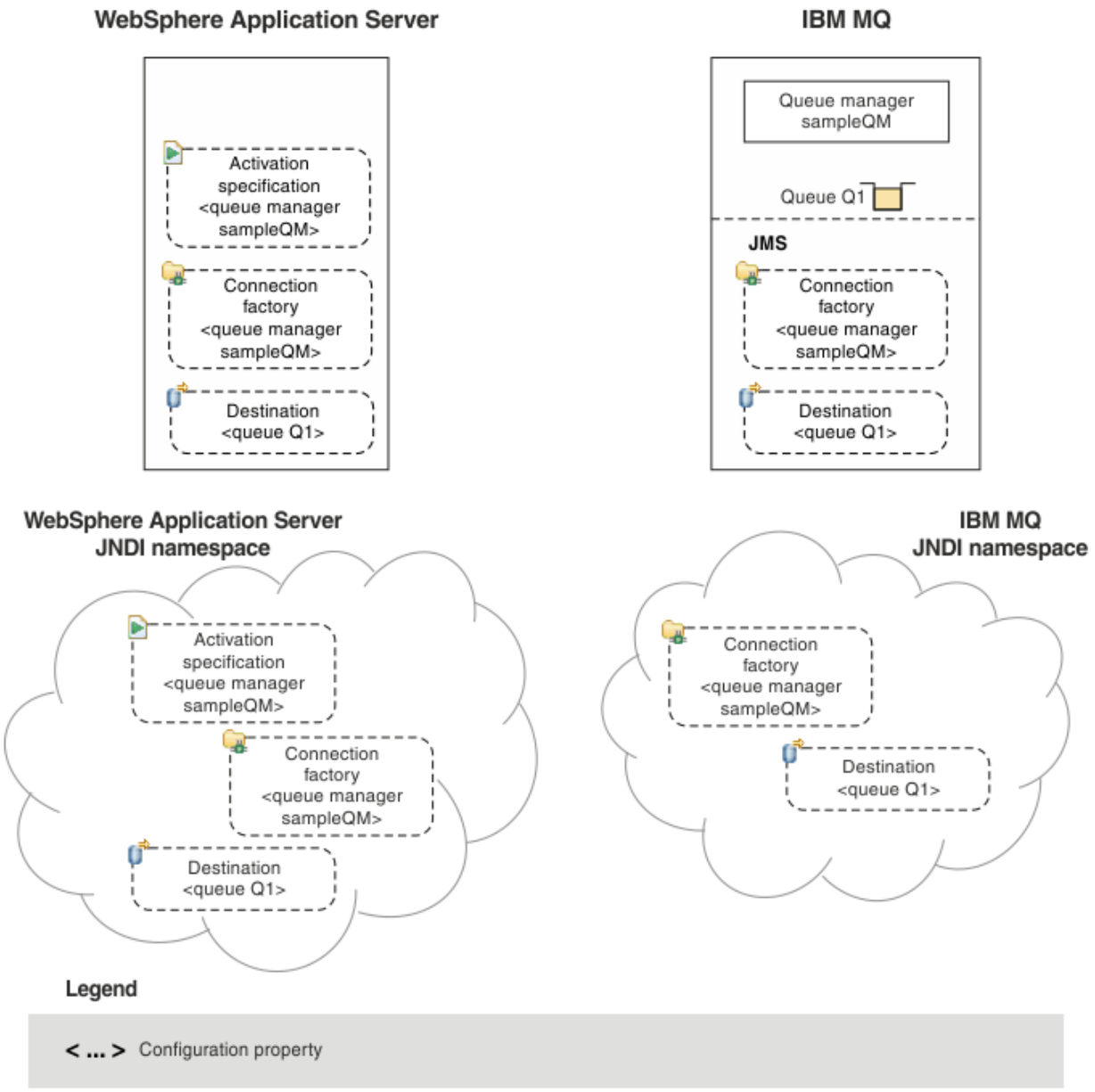
- Místo určení fronty JMS použité v dvoubodovém systému zpráv
- Místo určení tématu JMS použité v systému zpráv publikování/odběru

Následující diagram ukazuje příklad objektů produktu JMS vytvořených v oboru názvů JNDI produktu IBM MQ .



Obrázek 89. Objekty JMS vytvořené v produktu IBM MQ

Pokud používáte systém zpráv produktu JMS mezi produkty WebSphere Application Server a IBM MQ, musíte vytvořit odpovídající objekty v produktu WebSphere Application Server , které budou použity ke komunikaci s produktem IBM MQ. Při vytváření jednoho z těchto objektů v produktu WebSphere Application Serverje tento objekt uložen v oboru názvů rozhraní JNDI produktu WebSphere Application Server , jak je uvedeno v následujícím diagramu.



Obrázek 90. Objekty vytvořené v produktu WebSphere Application Servera odpovídající objekty v produktu IBM MQ

Pokud vaše aplikace používá objekt MDB (Message-driven bean), bude továrna připojení použita pouze pro odchozí zprávy a příchozí zprávy jsou přijímány specifikací aktivace. Specifikace aktivace jsou součástí standardu Java EE Connector Architecture 1.5 (JCA 1.5). Produkt JCA 1.5 poskytuje standardní způsob integrace poskytovatelů produktu JMS , jako je například produkt IBM MQ, s aplikačními servery Java EE , jako je například produkt WebSphere Application Server. Specifikace aktivace JMS může být přidružena k jednomu nebo více objektům typu message-driven bean (MDB) a poskytuje konfiguraci nezbytnou pro příjem těchto objektů MDB pro zprávy přicházející do místa určení.

K vytvoření a konfiguraci prostředků produktu JMS , které potřebujete, můžete použít buď administrativní konzolu produktu WebSphere Application Server , nebo skriptovací příkazy wsadmin.

Procedura

- Chcete-li nakonfigurovat objekty produktu JMS pro prostor IBM MQ pomocí produktu IBM MQ Explorer, viz “Konfigurace objektů produktu JMS pomocí produktu IBM MQ Explorer” na stránce 615.

- Chcete-li nakonfigurovat objekty produktu JMS pro prostor IBM MQ pomocí nástroje pro administraci produktu IBM MQ JMS , přečtěte si téma “Konfigurace objektů produktu JMS pomocí nástroje pro administraci” na stránce 616.
- Chcete-li konfigurovat objekty JMS pro produkt WebSphere Application Server, viz “Konfigurace prostředků produktu JMS v produktu WebSphere Application Server” na stránce 625.

Výsledky

Aplikace produktu IBM MQ classes for JMS může načíst spravované objekty z oboru názvů rozhraní JNDI a v případě potřeby nastavit nebo změnit jednu či více vlastností pomocí rozšíření produktu IBM JMS nebo rozšíření produktu IBM MQ JMS .

Související úlohy

Použití JNDI k načtení spravovaných objektů v aplikaci JMS

Vytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS

Konfigurace objektů produktu JMS pomocí produktu IBM MQ Explorer

Pomocí grafického uživatelského rozhraní produktu IBM MQ Explorer vytvořte objekty produktu JMS z objektů IBM MQ a objekty IBM MQ z objektů JMS a také pro administraci a monitorování dalších objektů produktu IBM MQ .

Informace o této úloze

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. Produkt IBM MQ Explorer lze provozovat v systémech Windows a Linux x86-64. Může se vzdáleně připojovat ke správcům front spuštěným na jakékoli podporované platformě včetně produktu z/OS, a umožnit tak zobrazení, prozkoumané a pozměňování celé komunikační páteře systému zpráv z konzoly.

V produktu IBM MQ Explorerjsou všechny továrny připojení uloženy ve složkách Továrny připojení v příslušném kontextu a dílčích kontextech.

Můžete provádět následující typy úloh s produktem IBM MQ Explorer, buď kontextově z existujícího objektu v produktu IBM MQ Explorer, nebo v rámci průvodce vytvořením nového objektu:

- Vytvořte továrnu připojení produktu JMS z libovolného z následujících objektů produktu IBM MQ :
  - Správce front produktu IBM MQ , ať už na lokálním počítači nebo na vzdáleném systému.
  - Kanál IBM MQ .
  - Modul listener produktu IBM MQ .
- Přidejte správce front IBM MQ do produktu IBM MQ Explorer pomocí továrny připojení produktu JMS .
- Vytvořte frontu JMS z fronty IBM MQ .
- Vytvořte frontu IBM MQ z fronty JMS .
- Vytvoření tématu JMS z tématu IBM MQ , které může být objektem IBM MQ nebo dynamickým tématem.
- Vytvoření tématu IBM MQ z tématu JMS .

Procedura

- Spusťte produkt IBM MQ Explorer, pokud již není spuštěn.

  Je-li produkt IBM MQ Explorer spuštěn a zobrazí úvodní stránku, zavřete úvodní stránku a spusťte administraci objektů produktu IBM MQ .
- Pokud jste tak dosud neučinili, vytvořte počáteční kontext definující kořenový adresář oboru názvů JNDI, ve kterém jsou objekty JMS uloženy ve službě pro správu pojmenování a adresářů.

  Po přidání počátečního kontextu do produktu 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 je-li zobrazen úplný obsah oboru názvů JNDI, v produktu IBM MQ Explorer můžete upravovat pouze objekty IBM MQ classes for JMS , které jsou uloženy zde. Další informace naleznete v tématu Přidání počátečního kontextu.

- Vytvořte a nakonfigurujte dílčí kontexty a spravované objekty JMS , které potřebujete.

  Další informace naleznete v tématu Vytvoření a konfigurace spravovaných objektů platformy JMS.
- Nakonfigurujte prostor IBM MQ.

  Další informace naleznete v tématu Konfigurace produktu IBM MQ pomocí produktu IBM MQ Explorer .

Související pojmy

Úvod do produktu IBM MQ Explorer

Související úlohy

Vytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS

Konfigurace objektů produktu JMS pomocí nástroje pro administraci

Pomocí nástroje pro administraci produktu IBM MQ JMS můžete definovat vlastnosti osmi typů objektů IBM MQ classes for JMS a uložit je do oboru názvů rozhraní JNDI. Aplikace pak mohou používat rozhraní JNDI k načtení těchto spravovaných objektů z oboru názvů.

Informace o této úloze

V následující tabulce jsou uvedeny osm typů spravovaných objektů, které lze vytvářet, konfigurovat a manipulovat s použitím příkazových slov. Sloupec Klíčové slovo zobrazuje řetězce, které můžete nahradit pro *TYPE* v příkazech zobrazených v Tabulka 37 na stránce 616.

Tabulka 37. Typy objektů produktu JMS , které jsou zpracovány nástrojem pro administraci

Typ objektu	**Klíčové slovo**	**Popis**
MQConnectionFactory	CF	Implementace rozhraní IBM MQ rozhraní ConnectionFactory produktu JMS . Představuje objekt továrny pro vytvoření připojení v doménách typu point-to-point i publikování/odběr.
Továrna MQQueueConnection	QCF	Implementace produktu IBM MQ rozhraní továrny produktu JMS QueueConnection. To představuje objekt továrny pro vytvoření připojení v doméně dvoubodového spojení.
Továrna MQTopicConnection	TCF	Implementace produktu IBM MQ rozhraní továrny JMS TopicConnection. Tento objekt představuje objekt továrny pro vytváření připojení v doméně publikování/odběru.
MQQUEUE	Q	The IBM MQ implementation of the JMS Queue interface. Představuje místo určení pro zprávy v rámci domény typu point-to-point.
MQTopic	T	Implementace produktu IBM MQ rozhraní tématu produktu JMS . Představuje místo určení pro zprávy v doméně publikování/odběru.

Tabulka 37. Typy objektů produktu JMS , které jsou zpracovány nástrojem pro administraci (pokračování)		
Typ objektu	**Klíčové slovo**	**Popis**
MQXAConnectionFactory “1” na stránce 617	XACF	Implementace rozhraní IBM MQ rozhraní JMS XAConnectionFactory . Představuje objekt továrny pro vytvoření připojení v doménách typu point-to-point i publikování/odběr a kde připojení používají verze XA pro třídy JMS .
Továrna MQXAQueueConnectionFactory “1” na stránce 617	XAQCF	Implementace produktu IBM MQ rozhraní továrny produktu JMS XAQueueConnection. Představuje objekt továrny pro vytvoření připojení v doméně dvoubodového spojení, které používají verze XA JMS tříd.
Továrna MQXATopicConnectionFactory “1” na stránce 617	XATCF	Implementace produktu IBM MQ rozhraní továrny produktu JMS XATopicConnection. Představuje objekt továrny pro vytváření připojení v doméně publikování/odběru, které používají verze XA pro JMS .

Poznámka:

1. Tyto třídy jsou k dispozici pro použití od dodavatelů aplikačních serverů. Je nepravděpodobné, že by byly pro programátory aplikací přímo užitečné.

Další informace o tom, jak nakonfigurovat tyto objekty, viz “Konfigurace objektů produktu JMS” na stránce 624.

Typy vlastností a hodnoty, které je třeba použít k použití tohoto nástroje, jsou uvedeny v části Vlastnosti objektů IBM MQ classes for JMS.

Tento nástroj můžete také použít k manipulaci s podkontexty oboru názvů adresáře v rámci rozhraní JNDI, jak je popsáno v tématu “Konfigurace dílčích kontextů” na stránce 621.

Objekty spravované produktem JMS můžete také vytvářet a konfigurovat pomocí produktu IBM MQ Explorer.

Související úlohy

Vytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS

Použití JNDI k načtení spravovaných objektů v aplikaci JMS

Konfigurace nástroje pro administraci produktu JMS

Nástroj pro administraci produktu IBM MQ JMS používá konfigurační soubor k nastavení hodnot určitých vlastností. K dispozici je ukázkový konfigurační soubor, který můžete upravit, aby vyhovoval vašemu systému.

Informace o této úloze

Konfigurační soubor je prostý textový soubor, který se skládá ze sady dvojic klíč-hodnota oddělených znakem rovnítka (=). Administrační nástroj nakonfigurujete nastavením hodnot pro tři vlastnosti definované v konfiguračním souboru. Následující příklad zobrazuje tyto tři vlastnosti:

```
#Set the service provider
INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
#Set the initial context
PROVIDER_URL=ldap://polaris/o=ibm_us,c=us
```

```
#Set the authentication type
SECURITY_AUTHENTICATION=none
```

(V tomto příkladu znak křížek (#) v prvním sloupci řádku označuje komentář, nebo řádek, který se nepoužívá.)

Ukázkový konfigurační soubor, který se používá jako výchozí konfigurační soubor, se dodává spolu s produktem IBM MQ. Ukázkový soubor se nazývá `JMSAdmin.config`a nachází se v adresáři *MQ_JAVA_INSTALL_PATH*`/bin` . Buď můžete tento ukázkový soubor upravit, abyste definovali nastavení potřebná pro váš systém, nebo můžete vytvořit svůj vlastní konfigurační soubor.

Když spustíte nástroj pro administraci, můžete uvést konfigurační soubor, který chcete použít, pomocí parametru příkazového řádku `-cfg` , jak je popsáno v “Spuštění nástroje pro administraci” na stránce 619. Pokud při vyvolání nástroje nezadáte název konfiguračního souboru, nástroj se pokusí načíst výchozí konfigurační soubor (`JMSAdmin.config`). Prohledává tento soubor jako první v aktuálním adresáři a potom v adresáři *MQ_JAVA_INSTALL_PATH*`/bin` , kde *MQ_JAVA_INSTALL_PATH* je cesta k vaší instalaci produktu IBM MQ classes for JMS .

Názvy objektů produktu JMS , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jedním z těchto konvencí je, že názvy objektu a kontextu musí obsahovat předponu, jako například `cn=` (obecný název) nebo `ou=` (organizační jednotka). Administrační nástroj zjednodušuje použití poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který dodáte. Pro protokol LDAP je to `cn=`. Je-li to nutné, můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru.

Poznámka: Možná budete muset nakonfigurovat server LDAP pro ukládání objektů Java . Další informace naleznete v dokumentaci k serveru LDAP.

Postup

1. Definujte poskytovatele služeb, kterého nástroj používá, konfigurací vlastnosti **INITIAL_CONTEXT_FACTORY** .

   Podporované hodnoty této vlastnosti jsou následující:

   - com.sun.jndi.ldap.LdapCtxFactory (pro LDAP)
   - com.sun.jndi.fscontext.RefFSContextFactory (pro kontext systému souborů)
   - z/OS com.ibm.jndi.LDAPCtxFactory je podporováno pouze v systému z/OS a poskytuje přístup k serveru LDAP. Tato třída je však nekompatibilní s hodnotou com.sun.jndi.ldap.LdapCtxFactoryv tom, že objekty vytvořené pomocí jednoho objektu InitialContextFactory nelze číst nebo upravovat pomocí druhé.

   Administrační nástroj lze také použít k připojení k jiným kontextům rozhraní JNDI pomocí tří parametrů definovaných v konfiguračním souboru JMSAdmin. Chcete-li použít jinou továrnu InitialContext, postupujte takto:

   a) Nastavte vlastnost **INITIAL_CONTEXT_FACTORY** na požadovaný název třídy.

   b) Definujte chování továrny InitialContextFactory pomocí vlastností **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** a **NAME_READABILITY_MARKER** .

      Nastavení pro tyto vlastnosti jsou popsány v komentářích ukázkového konfiguračního souboru.

   Pokud použijete některou z podporovaných hodnot **INITIAL_CONTEXT_FACTORY** , není třeba definovat vlastnosti **USE_INITIAL_DIR_CONTEXT**, **NAME_PREFIX** a **NAME_READABILITY_MARKER** . Chcete-li však přepsat výchozí nastavení systému, můžete těmto vlastnostem dát hodnoty, chcete-li potlačit výchozí nastavení systému. Pokud jsou například vaše objekty uloženy v prostředí LDAP, můžete změnit výchozí předponu, kterou nástroj přidá k objektům a kontextovým názvům, nastavením vlastnosti **NAME_PREFIX** na požadovanou předponu.

   Vynecháte-li jeden nebo více z těchto tří vlastností továrny InitialContext, nástroj pro administraci poskytne vhodné výchozí hodnoty založené na hodnotách ostatních vlastností.
2. Definujte adresu URL počátečního kontextu relace nakonfigurováním vlastnosti **PROVIDER_URL** .

Tato adresa URL je kořenem všech operací rozhraní JNDI, které nástroj provádí. Jsou podporovány dvě formy této vlastnosti:

- ldap://název_hostitele/kontextový_název
- file: [jednotka:] /název_cesty

Formát adresy URL protokolu LDAP se může lišit v závislosti na poskytovateli LDAP. Další informace naleznete v dokumentaci k protokolu LDAP.

3. Definujte, zda rozhraní JNDI předá pověření zabezpečení poskytovateli služeb nakonfigurováním vlastnosti **SECURITY_AUTHENTICATION** .

   Tato vlastnost se používá pouze tehdy, je-li použit poskytovatel služby LDAP a může mít jednu ze tří hodnot:

   žádná (anonymní ověření)
   Nastavíte-li tento parametr na hodnotu none, rozhraní JNDI nepředá žádné pověření zabezpečení poskytovateli služby a provede se *anonymní ověření* .

   simple (jednoduché ověření)
   Nastavíte-li tento parametr na hodnotu simple, budou pověření zabezpečení předávána prostřednictvím rozhraní JNDI základního poskytovatele služeb. Tato bezpečnostní pověření jsou ve formě rozlišovacího jména uživatele (DN uživatele) a hesla.

   CRAM-MD5 (mechanizmus ověřeníCRAM-MD5)
   Nastavíte-li tento parametr na hodnotu CRAM-MD5, budou pověření zabezpečení předávána prostřednictvím rozhraní JNDI základního poskytovatele služeb. Tato bezpečnostní pověření jsou ve formě rozlišovacího jména uživatele (DN uživatele) a hesla.

   Pokud nezadáte platnou hodnotu pro vlastnost **SECURITY_AUTHENTICATION** , výchozí hodnota vlastnosti je none.

   Jsou-li požadována pověření zabezpečení, budete při inicializaci nástroje vyzváni k jejich zadání. Tomuto se lze vyhnout nastavením vlastností **PROVIDER_USERDN** a **PROVIDER_PASSWORD** v konfiguračním souboru JMSAdmin.

   Poznámka: Pokud tyto vlastnosti nepoužijete, vypíše se na obrazovku text zadaný *včetně hesla*. To může mít dopad na zabezpečení.

   Nástroj neprovádí žádné ověření; úloha ověření je delegována na server LDAP. Administrátor serveru LDAP musí nastavit a udržovat přístupová oprávnění k různým částem adresáře. Další informace naleznete v dokumentaci k protokolu LDAP. Pokud ověření selže, nástroj zobrazí odpovídající chybovou zprávu a ukončí se.

   Podrobnější informace o zabezpečení a rozhraní JNDI najdete v dokumentaci na webových stránkách Oracle' s Java (Oracle Technology Network for Java Developers).

Spuštění nástroje pro administraci

Nástroj pro administraci má rozhraní příkazového řádku, které můžete použít buď interaktivně, nebo spustit dávkové zpracování.

Informace o této úloze

Interaktivní režim poskytuje příkazový řádek, kde můžete zadat příkazy administrace. V dávkovém režimu obsahuje příkaz ke spuštění nástroje název souboru, který obsahuje příkazový skript administrace.

Procedura

Interaktivní režim

- Chcete-li spustit nástroj v interaktivním režimu, zadejte tento příkaz:

```
JMSAdmin [-t] [-v] [-cfg config_filename]
```

kde:

-t
Povolí trasování (výchozí je trasování vypnuto).

Trasovací soubor je generován v produktu `"%MQ_JAVA_DATA_PATH%"\errors` (Windows) nebo `/var/mqm/trace` (UNIX). Název trasovacího souboru je ve tvaru:

`mqjms_`*`PID`*`.trc`

kde *PID* je ID procesu prostředí JVM.

-v
Produkuje výstup s komentářem (výchozí hodnota je terse output)

-cfg název_konfiguračního_souboru
Název alternativního konfiguračního souboru. Je-li tento parametr vynechán, použije se výchozí konfigurační soubor `JMSAdmin.config`. Další informace o konfiguračním souboru viz téma “Konfigurace nástroje pro administraci produktu JMS” na stránce 617.

Zobrazí se příkazový řádek, který označuje, že je nástroj připraven přijímat příkazy administrace. Tato výzva se nejprve zobrazí jako:

```
InitCtx>
```

indikující, že aktuální kontext (tj. kontext JNDI, ke kterému se momentálně odkazují všechny operace pojmenovávání a adresářů), je počáteční kontext definovaný v konfiguračním parametru **PROVIDER_URL** . Další informace o tomto parametru naleznete v části “Konfigurace nástroje pro administraci produktu JMS” na stránce 617.

Při procházení oboru názvů adresáře se výzva k zobrazení této výzvy projeví, takže výzva k zadání vždy zobrazí aktuální kontext.

Dávkový režim

- Chcete-li spustit nástroj v dávkovém režimu, zadejte tento příkaz:

```
JMSAdmin test.scp
```

kde *test.scp* je skriptový soubor, který obsahuje příkazy administrace. Další informace viz “Použití příkazů administrace” na stránce 620. Poslední příkaz v souboru musí být příkaz END .

Použití příkazů administrace

Nástroj pro správu přijímá příkazy skládající se z příkazového slova a jeho příslušných parametrů.

Informace o této úloze

Následující tabulka obsahuje seznam administrativních příkazových slov, které lze použít při zadávání příkazů s použitím administračního nástroje.

Tabulka 38. Příkazová slova

Sloveso	**Krátký formát**	**Popis**
ALTER	KLÁVESA ALT	Změnit alespoň jednu z vlastností spravovaného objektu
Definice	DEF	Vytvoření a uložení spravovaného objektu nebo vytvoření dílčího kontextu
DISPLAY	DIS	Zobrazit vlastnosti jednoho nebo více uložených spravovaných objektů nebo obsah aktuálního kontextu
ODSTRANIT	DEL	Odebrat jeden nebo více spravovaných objektů z oboru názvů nebo odebrat prázdný podkontext

Tabulka 38. Příkazová slova (pokračování)		
Sloveso	**Krátký formát**	**Popis**
CHANGE	chg	Pozměnit aktuální kontext tak, aby uživatel mohl procházet obor názvů adresáře kdekoli pod počátečním kontextem (nevyřízená bezpečnostní prověrka)
COPY	CP	Vytvořit kopii uloženého spravovaného objektu a uložit jej pod alternativní název
MOVE	MV	Změnit název, pod kterým je spravovaný objekt uložen.
END		Zavřete nástroj pro administraci.

Procedura

- Není-li administrační nástroj již spuštěn, spusťte jej podle popisu v části "Spuštění nástroje pro administraci" na stránce 619.

  Zobrazí se příkazový řádek, který označuje, že nástroj je připraven přijmout příkazy administrace. Tato výzva se nejprve zobrazí jako:

  ```
  InitCtx>
  ```

  Chcete-li změnit aktuální kontext, použijte příkaz CHANGE , jak je popsáno v tématu "Konfigurace dílčích kontextů" na stránce 621.
- Zadejte příkazy v následujícím tvaru:

  ```
  verb [param]*
  ```

  kde **verb** je jedním z administračních příkazových slov uvedených v Tabulka 38 na stránce 620. Všechny platné příkazy obsahují jedno příkazové slovo, které se objevuje na začátku příkazu buď ve standardním, nebo v krátkém tvaru. Názvy příkazů Verb nejsou citlivé na velikost písmen.
- Chcete-li ukončit příkaz, stiskněte klávesu Enter, pokud nechcete zadat několik příkazů najednou, v takovém případě zadejte znaménko plus (+) přímo před stisknutím klávesy Enter.

  Chcete-li příkazy ukončit, stiskněte klávesu Enter. Tuto operaci však můžete potlačit zadáním znaku plus (+) před stisknutím klávesy Enter. To vám umožní zadat víceřádkové příkazy, jak je zobrazeno v následujícím příkladu:

  ```
  DEFINE Q(BookingsInputQueue) +
  QMGR(QM.POLARIS.TEST) +
  QUEUE(BOOKINGS.INPUT.QUEUE) +
  PORT(1415) +
  CCSID(437)
  ```
- Chcete-li zavřít nástroj pro administraci, použijte příkazové slovo **END** .

  Toto slovo nemůže obsahovat žádné parametry.

Konfigurace dílčích kontextů

Chcete-li konfigurovat dílčí kontexty oboru názvů adresáře, můžete použít příkazy **CHANGE**, **DEFINE**, **DISPLAY** a **DELETE** .

Informace o této úloze

Použití těchto příkazových slov je popsáno v následující tabulce.

Tabulka 39. Syntaxe a popis příkazů používaných k manipulaci s podkontexty	
Syntaxe příkazu	**Popis**
DEFINE CTX (ctxName)	Pokusí se o vytvoření podřízeného dílčího kontextu aktuálního kontextu s názvem ctxName. Pokud již existuje narušení zabezpečení, dojde k selhání zabezpečení, pokud již existuje, nebo není-li zadaný název platný.
ZOBRAZIT CTX	Zobrazí obsah aktuálního kontextu. Spravované objekty jsou anotovány pomocí a, dílčích kontextů s `[D]`. Zobrazí se také typ Java každého objektu.
ODSTRANIT CTX (ctxName)	Pokusy o odstranění podřízeného kontextu aktuálního kontextu s názvem ctxName. Pokud kontext nebyl nalezen, je neprázdný kontext nebo došlo k narušení zabezpečení.
CHANGE CTX (ctxName)	Pozměňuje aktuální kontext, takže se nyní odkazuje na podřízený kontext s názvem ctxName. Je možné zadat jednu ze dvou speciálních hodnot ctxName : **= NAHORU** přesunout na nadřízený prvek aktuálního kontextu **= INICIALIZACE** přesun přímo do počátečního kontextu Selhání, pokud určený kontext neexistuje, nebo pokud došlo k narušení zabezpečení.

Názvy objektů produktu JMS , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jedním z těchto konvencí je, že názvy objektu a kontextu musí obsahovat předponu, jako například `cn=` (obecný název) nebo `ou=` (organizační jednotka). Administrační nástroj zjednodušuje použití poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který dodáte. Pro protokol LDAP je to `cn=`. Je-li to nutné, můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru. Další informace viz “Konfigurace nástroje pro administraci produktu JMS” na stránce 617.

Poznámka: Možná budete muset nakonfigurovat server LDAP pro ukládání objektů Java . Další informace naleznete v dokumentaci k serveru LDAP.

Vytváření objektů JMS

Chcete-li vytvořit továrnu připojení JMS a cílové objekty a uložit je do oboru názvů JNDI, použijte příkazové slovo `DEFINE` . Chcete-li ukládat své objekty v prostředí LDAP, musíte jim dát názvy, které odpovídají určitým konvencím. Administrativní nástroj vám může pomoci dodržovat konvence pojmenování LDAP tím, že přidáte výchozí předponu k názvům objektů.

Informace o této úloze

Příkaz DEFINE vytváří administrovaný objekt s typem, názvem a vlastnostmi, které jste zadali. Nový objekt je uložen v aktuálním kontextu.

Názvy objektů produktu JMS , které jsou uloženy v prostředí LDAP, musí odpovídat konvencím pojmenování LDAP. Jedním z těchto konvencí je, že názvy objektu a kontextu musí obsahovat předponu, jako například `cn=` (obecný název) nebo `ou=` (organizační jednotka). Administrační nástroj zjednodušuje použití poskytovatelů služeb LDAP tím, že vám umožňuje odkazovat na názvy objektů a kontextů bez předpony. Pokud nezadáte předponu, nástroj automaticky přidá výchozí předponu k názvu, který dodáte. Pro protokol LDAP je to `cn=`. Je-li to nutné, můžete výchozí předponu změnit nastavením vlastnosti **NAME_PREFIX** v konfiguračním souboru. Další informace viz “Konfigurace nástroje pro administraci produktu JMS” na stránce 617.

Poznámka: Možná budete muset nakonfigurovat server LDAP pro ukládání objektů Java . Další informace naleznete v dokumentaci k serveru LDAP.

Postup

1. Není-li administrační nástroj již spuštěn, spusťte jej podle popisu v části “Spuštění nástroje pro administraci” na stránce 619.

   Zobrazí se příkazový řádek, který označuje, že nástroj je připraven přijmout příkazy administrace.
2. Ujistěte se, že příkazový řádek zobrazuje kontext, ve kterém chcete vytvořit nový objekt.

   Po spuštění nástroje pro administraci se na počátku zobrazí výzva k zadání jako:

   ```
   InitCtx>
   ```

   Chcete-li změnit aktuální kontext, použijte příkaz CHANGE , jak je popsáno v tématu “Konfigurace dílčích kontextů” na stránce 621.
3. Chcete-li vytvořit továrnu připojení, místo určení fronty nebo cíl tématu, použijte následující syntaxi příkazu:

   ```
   DEFINE TYPE (name) [property]*
   ```

   To znamená, že zadáte příkaz DEFINE a za ním následuje odkaz na spravovaný objekt *TYPE* （name）, následovaný nulou nebo více *vlastnostmi* (viz Vlastnosti objektů IBM MQ classes for JMS).
4. Chcete-li vytvořit továrnu připojení, místo určení fronty nebo cíl tématu, použijte následující syntaxi příkazu:

   ```
   DEFINE TYPE (name) [property]*
   ```
5. Chcete-li zobrazit nově vytvořený objekt, použijte příkazové slovo DISPLAY s následující syntaxí příkazu:

   ```
   DISPLAY TYPE (name)
   ```

Příklad

Následující příklad ukazuje frontu s názvem testQueue vytvořenou v počátečním kontextu pomocí příkazu DEFINE . Vzhledem k tomu, že tento objekt je ukládán v prostředí LDAP, ačkoli název objektu testQueue není zadán s předponou, nástroj automaticky přidá jeden k zajištění shody s konvencemi pojmenování LDAP. Zadání příkazu DISPLAY Q(testQueue) také způsobí, že se přidá tato předpona.

```
InitCtx> DEFINE Q(testQueue)

InitCtx> DISPLAY CTX

Contents of InitCtx

a cn=testQueue       com.ibm.mq.jms.MQQueue

1 Object(s)
0 Context(s)
1 Binding(s), 1 Administered
```

Ukázkové chybové stavy vytvářející objekt JMS

Při vytváření objektu může vzniknout řada běžných chybových stavů.

Zde jsou příklady těchto chybových stavů:

CipherSpec mapována na CipherSuite

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SSLCIPHERSUITE(RC4_MD5_US)
WARNING: Converting CipherSpec RC4_MD5_US to
CipherSuite SSL_RSA_WITH_RC4_128_MD5
```

Neplatná vlastnost pro objekt

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PRIORITY(4)
Unable to create a valid object, please check the parameters supplied
Invalid property for a QCF: PRI
```

Neplatný typ hodnoty vlastnosti

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) CCSID(english)
Unable to create a valid object, please check the parameters supplied
Invalid value for CCS property: English
```

Konflikt vlastností-klient/bin.

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) HOSTNAME(polaris.hursley.ibm.com)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: Client-bindings attribute clash
```

Konflikt vlastností-inicializace uživatelské procedury

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) SECEXITINIT(initStr)
Unable to create a valid object, please check the parameters supplied
Invalid property in this context: ExitInit string supplied
without Exit string
```

Hodnota vlastnosti mimo platný rozsah

```
InitCtx/cn=Trash> DEFINE Q(testQ) PRIORITY(12)
Unable to create a valid object, please check the parameters supplied
Invalid value for PRI property: 12
```

Neznámá vlastnost

```
InitCtx/cn=Trash> DEFINE QCF(testQCF) PIZZA(ham and mushroom)
Unable to create a valid object, please check the parameters supplied
Unknown property: PIZZA
```

Níže jsou uvedeny příklady chybových stavů, které se mohou objevit na produktu Windows při vyhledávání spravovaných objektů JNDI z aplikace produktu JMS .

1. Pokud používáte poskytovatele JNDI WebSphere , com.ibm.websphere.naming.WsnInitialContextFactory, musíte použít dopředné lomítko (/) pro přístup ke spravovaným objektům definovaným v dílčích kontextech; například jms/MyQueueNázev. Použijete-li zpětné lomítko (\), dojde k výjimce InvalidName.
2. Používáte-li poskytovatele JNDI Oracle , com.sun.jndi.fscontext.RefFSContextFactory, musíte použít zpětné lomítko (\) pro přístup ke spravovaným objektům definovaným v dílčích kontextech; například ctx1\\fred. Použijete-li dopředné lomítko (/), dojde k NameNotFoundException .

Konfigurace objektů produktu JMS

Chcete-li manipulovat se spravovanými objekty v oboru názvů adresáře, můžete použít příkazy ALTER, DEFINE, DISPLAY, DELETE, COPYa MOVE .

Informace o této úloze

Tabulka 40 na stránce 625 shrnuje použití těchto příkazových slov. Nahraďte *TYPE* klíčovým slovem, které představuje požadovaný spravovaný objekt, jak je popsáno v “Konfigurace objektů produktu JMS pomocí nástroje pro administraci” na stránce 616.

Tabulka 40. Syntaxe a popis příkazů používaných k manipulaci se spravovanými objekty

Syntaxe příkazu	**Popis**
ALTER *TYPE* (název) [vlastnost] *	Pokusí se aktualizovat vlastnosti administrovaného objektu s dodanými objekty. Pokud došlo k narušení zabezpečení, selhání v případě, že uvedený objekt nebyl nalezen, nebo nejsou-li zadané nové vlastnosti platné.
DEFINE *TYP* (název) [vlastnost] *	Pokouší se vytvořit spravovaný objekt typu *TYPE* s dodanými vlastnostmi a uložit jej pod názvem name v aktuálním kontextu. Pokud je poskytnutý název neplatný nebo objekt s daným názvem existuje, nebo pokud zadané vlastnosti nejsou platné, došlo k selhání zabezpečení.
DISPLAY *TYP* (název)	Zobrazí vlastnosti spravovaného objektu typu *TYPE* s vazbou pod názvem name v aktuálním kontextu. Selhání, pokud objekt neexistuje, nebo pokud došlo k narušení zabezpečení.
DELETE *TYPE* (název)	Pokusí se odebrat administrovaný objekt typu *TYPE* , který má název name, z aktuálního kontextu. Selhání, pokud objekt neexistuje, nebo pokud došlo k narušení zabezpečení.
COPY *TYP* (nameA) *TYP* (nameB)	Vytvoří kopii spravovaného objektu typu *TYPE* s názvem nameAa pojmenovává se kopie nameB. Toto vše se vyskytuje v rozsahu aktuálního kontextu. Pokud objekt, který má být kopírován, neexistuje, existuje-li objekt s názvem nameB , nebo pokud dojde k narušení zabezpečení.
MOVE *TYPE* (nameA) *TYP* (nameB)	Přesouvá (přejmenovává) spravovaný objekt typu *TYPE* s názvem nameAna nameB. Toto vše se vyskytuje v rozsahu aktuálního kontextu. Pokud objekt, který má být přesunut, neexistuje, existuje-li objekt s názvem nameB , nebo pokud došlo k narušení zabezpečení.

Konfigurace prostředků produktu JMS v produktu WebSphere Application Server

Chcete-li konfigurovat prostředky produktu JMS v produktu WebSphere Application Server, můžete buď použít administrativní konzolu, nebo příkazy wsadmin.

Informace o této úloze

Aplikace produktu Java Message Service (JMS) obvykle závisí na externě nakonfigurovaných objektech, které popisují způsob, jakým se aplikace připojuje ke svému poskytovateli JMS a k místům určení, ke kterým přistupuje. Aplikace produktu JMS používají produkt Java Naming Directory Interface (JNDI) k přístupu k následujícím typům objektů za běhu:

- Specifikace aktivace (používané aplikačními servery Java EE)
- Unifikované továrny připojení (s produktem JMS 1.1, továrny na připojení nezávislé na doméně (unifikované) jsou preferovány továrny připojení fronty specifické pro konkrétní doménu a továrny připojení témat)
- Továrny připojení tématu (používané aplikacemi produktu JMS 1.0)
- Továrny připojení fronty (používané aplikacemi produktu JMS 1.0)

- Fronty
- Témata

Through the IBM MQ messaging provider in WebSphere Application Server, Java Message Service (JMS) messaging applications can use your IBM MQ system as an external provider of JMS messaging resources. Chcete-li tento přístup povolit, nakonfigurujte poskytovatele systému zpráv produktu IBM MQ v produktu WebSphere Application Server za účelem definování prostředků produktu JMS pro připojení k libovolnému správci front v síti produktu IBM MQ .

Produkt WebSphere Application Server můžete použít ke konfiguraci prostředků produktu IBM MQ pro aplikace (například továrny připojení fronty) a ke správě zpráv a odběrů asociovaných s místy určení JMS . Zabezpečení budete spravovat prostřednictvím produktu IBM MQ.

Související úlohy

Společně s IBM MQ a WebSphere Application Server

WebSphere Application Server Témata

Interoperace pomocí poskytovatele systému zpráv produktu IBM MQ

Správa systému zpráv s poskytovatelem systému zpráv produktu IBM MQ

Mapování názvů panelů administrativní konzoly na názvy příkazů a názvy IBM MQ

Konfigurace prostředků produktu JMS pomocí administrativní konzoly

Administrativní konzolu produktu WebSphere Application Server můžete použít ke konfiguraci specifikací aktivace, továren připojení a cílů pro poskytovatele IBM MQ JMS .

Informace o této úloze

Administrativní konzolu produktu WebSphere Application Server můžete použít k vytvoření, zobrazení nebo úpravě libovolného z následujících prostředků:

- Specifikace aktivace
- Továrny na připojení nezávislé na doméně (JMS 1.1 nebo novější)
- Továrny připojení fronty
- Továrny připojení tématu
- Fronty
- Témata

Následující kroky poskytují přehled způsobů, jak pomocí administrativní konzoly konfigurovat prostředky produktu JMS pro použití s poskytovatelem systému zpráv produktu IBM MQ . Každý krok obsahuje název tématu v dokumentaci produktu WebSphere Application Server , na který se můžete podívat, abyste získali další informace. Odkazy na tato témata v dokumentaci produktu WebSphere Application Server viz *Související odkazy* .

V buňce se smíšenými verzemi produktu WebSphere Application Server můžete spravovat prostředky produktu IBM MQ v uzlech všech verzí. Některé vlastnosti však nejsou k dispozici ve všech verzích. V této situaci jsou v administrativní konzole zobrazeny pouze vlastnosti daného uzlu.

Procedura

Chcete-li vytvořit nebo konfigurovat specifikaci aktivace pro použití s poskytovatelem systému zpráv produktu IBM MQ , postupujte takto:

- Chcete-li vytvořit specifikaci aktivace, použijte průvodce vytvořením prostředku produktu IBM MQ JMS .

  Můžete buď použít průvodce k uvedení všech podrobností pro specifikaci aktivace, nebo můžete zvolit uvedení podrobností připojení pro IBM MQ pomocí tabulky CCDT (Client Channel Definition table). Když zadáte podrobnosti připojení pomocí průvodce, můžete zvolit buď zadání informací o hostiteli a portu samostatně, nebo, pokud používáte správce front s více instancemi, abyste mohli zadat

informace o hostiteli a portu ve formě seznamu názvů připojení. Další informace naleznete v tématu *Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ*.

- Chcete-li zobrazit nebo změnit vlastnosti konfigurace specifikace aktivace, použijte panel nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ k administrativní konzole.

  Tyto konfigurační vlastnosti řídí způsob vytváření připojení k přidruženým frontám a tématům. Další informace naleznete v tématu *Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li vytvořit nebo konfigurovat sjednocenou továrnu připojení, továrnu připojení fronty nebo továrnu připojení tématu pro použití s poskytovatelem systému zpráv produktu IBM MQ , postupujte takto:

- Chcete-li vytvořit továrnu na připojení, nejprve vyberte typ továrny připojení, který chcete vytvořit, a pak pomocí průvodce Vytvořit prostředek IBM MQ JMS určete podrobnosti.
  - Má-li aplikace JMS používat pouze dvoubodový systém zpráv, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv typu point-to-point, kterou lze použít pro vytváření připojení konkrétně pro systém zpráv typu point-to-point.
  - Je-li vaše aplikace produktu JMS určena pouze k použití systému zpráv publikování/odběru, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv publikování/odběru, kterou lze použít pro vytváření připojení speciálně pro systém zpráv publikování/odběru.
  - Pro produkt JMS 1.1 nebo novější vytvořte továrnu připojení nezávislou na doméně, kterou lze použít jak pro systém zpráv typu point-to-point, tak pro systém zpráv typu publikování/odběr, což umožňuje aplikaci provádět jak dvoubodové spojení, tak i publikování/odběr práce pod stejnou transakcí.

  Můžete zvolit, zda se má průvodce použít k zadání všech podrobností pro továrnu připojení, nebo můžete určit podrobnosti o připojení pro produkt IBM MQ pomocí tabulky CCDT (Client Channel Definition table). Když zadáte podrobnosti připojení pomocí průvodce, můžete zvolit buď zadání informací o hostiteli a portu samostatně, nebo, pokud používáte správce front s více instancemi, abyste mohli zadat informace o hostiteli a portu ve formě seznamu názvů připojení. Další informace naleznete v tématu *Vytvoření továrny na připojení pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li zobrazit nebo změnit vlastnosti konfigurace faktorie připojení, postupujte takto:

- Pro typ továrny připojení, který chcete konfigurovat, použijte panel nastavení továrny připojení konzoly pro správu.

  Konfigurační vlastnosti řídí způsob vytváření připojení k přidruženým frontám a tématům. Další informace naleznete v tématu *Konfigurace továrny na kolekce pro poskytovatele systému zpráv produktu IBM MQ*nebo *Konfigurace továrny kolekce fronty pro poskytovatele systému zpráv produktu IBM MQ*nebo *Konfigurace továrny kolekce témat pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li konfigurovat místo určení fronty JMS pro systém zpráv typu point-to-point s poskytovatelem systému zpráv produktu IBM MQ ,

- Panel nastavení fronty poskytovatele systému zpráv produktu IBM MQ administrativní konzoly slouží k definování následujících typů vlastností:
  - Obecné vlastnosti, včetně administračních a IBM MQ vlastností fronty.
  - Vlastnosti připojení, které určují způsob připojení ke správci front, který je hostitelem fronty.
  - Rozšířené vlastnosti, které řídí chování připojení k místům určení poskytovatele systému zpráv produktu IBM MQ .
  - Libovolné přizpůsobené vlastnosti pro místo určení fronty.

  Další informace naleznete v tématu *Konfigurace fronty pro poskytovatele systému zpráv produktu IBM MQ*.

Chcete-li vytvořit nebo nakonfigurovat místo určení tématu produktu JMS pro systém zpráv publikování/odběru s poskytovatelem systému zpráv produktu IBM MQ , postupujte takto:

- Panel nastavení tématu poskytovatele systému zpráv produktu IBM MQ slouží k definování následujících typů vlastností:
  - Obecné vlastnosti, včetně administrace a vlastností témat IBM MQ .

- Rozšířené vlastnosti, které řídí chování připojení k místům určení poskytovatele systému zpráv produktu IBM MQ .
- Libovolné přizpůsobené vlastnosti pro místo určení fronty.

Další informace naleznete v tématu *Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ*.

Související pojmy

“Správci front s více instancemi” na stránce 457
Správci front s více instancemi jsou instance stejného správce front konfigurovaného na různých serverech. Jedna instance správce front je definována jako aktivní instance a jiná instance je definována jako instance v pohotovostním režimu. Dojde-li k selhání aktivní instance, správce front s více instancemi se automaticky restartuje na záložním serveru.

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 381
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 produktu IBM MQ
Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ
Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ
Vytvoření továrny na připojení pro poskytovatele systému zpráv produktu IBM MQ
Konfigurace sjednocené továrny připojení pro poskytovatele systému zpráv produktu IBM MQ
Konfigurace továrny připojení fronty pro poskytovatele systému zpráv produktu IBM MQ
Konfigurace továrny připojení tématu pro poskytovatele systému zpráv produktu IBM MQ
Konfigurace fronty pro poskytovatele systému zpráv produktu IBM MQ
Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ

Konfigurace prostředků produktu JMS pomocí skriptovacích příkazů nástroje wsadmin

You can use WebSphere Application Server wsadmin scripting commands to create, modify, delete or show information about JMS activation specifications, connection factories, queues and topics. Můžete také zobrazit a spravovat nastavení pro adaptér prostředků produktu IBM MQ .

Informace o této úloze

Následující kroky poskytují přehled způsobů, jak pomocí příkazů wsadmin wsadmin WebSphere Application Server konfigurovat prostředky produktu JMS pro použití s poskytovatelem systému zpráv produktu IBM MQ . Další informace o způsobu použití těchto příkazů naleznete v tématu *Související odkazy* pro odkazy na dokumentaci produktu WebSphere Application Server .

Chcete-li spustit příkaz, použijte objekt AdminTask skriptovacího klienta wsadmin.

Po použití příkazu k vytvoření nového objektu nebo k provedení změn uložte provedené změny do hlavní konfigurace. Použijte například následující příkaz:

```
AdminConfig.save()
```

Chcete-li zobrazit seznam dostupných administrativních příkazů poskytovatele systému zpráv produktu IBM MQ a stručný popis jednotlivých příkazů, zadejte na příkazový řádek nástroje wsadmin následující příkaz:

```
print AdminTask.help('WMQAdminCommands')
```

Chcete-li zobrazit přehlednou nápovědu k danému příkazu, zadejte na příkazový řádek nástroje wsadmin následující příkaz:

```
print AdminTask.help('command_name')
```

Procedura

Chcete-li vypsat všechny prostředky poskytovatele systému zpráv produktu IBM MQ definované v oboru, ve kterém je příkaz zadán, použijte následující příkazy.

- Chcete-li vypsat specifikace aktivace, použijte příkaz **listWMQActivationSpecs** .
- Chcete-li vypsat seznam továren připojení, použijte příkaz **listWMQConnectionFactories** .
- Chcete-li vypsat cíle typu fronty, použijte příkaz **listWMQQueues** .
- Chcete-li zobrazit seznam míst určení typu tématu, použijte příkaz **listWMQTopics** .

Chcete-li vytvořit prostředek produktu JMS pro poskytovatele systému zpráv produktu IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li vytvořit specifikaci aktivace, použijte příkaz **createWMQActivationSpec** .

  Můžete buď vytvořit specifikaci aktivace zadáním všech parametrů, které mají být použity pro vytvoření připojení, nebo můžete vytvořit specifikaci aktivace tak, aby používala tabulku definic kanálů klienta (CCDT) k vyhledání správce front, k němuž se má připojit.
- Chcete-li vytvořit továrnu připojení, použijte příkaz **createWMQConnectionFactory** s použitím parametru **-type** k určení typu továrny připojení, kterou chcete vytvořit:
  - Má-li aplikace JMS používat pouze dvoubodový systém zpráv, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv typu point-to-point, kterou lze použít pro vytváření připojení konkrétně pro systém zpráv typu point-to-point.
  - Je-li vaše aplikace produktu JMS určena pouze k použití systému zpráv publikování/odběru, vytvořte továrnu připojení specifickou pro doménu pro doménu systému zpráv publikování/odběru, kterou lze použít pro vytváření připojení speciálně pro systém zpráv publikování/odběru.
  - Pro produkt JMS 1.1 nebo novější vytvořte továrnu připojení nezávislou na doméně, kterou lze použít jak pro systém zpráv typu point-to-point, tak pro systém zpráv typu publikování/odběr, což umožňuje aplikaci provádět jak dvoubodové spojení, tak i publikování/odběr práce pod stejnou transakcí.

  Výchozí typ je továrna připojení nezávislá na doméně.
- Chcete-li vytvořit místo určení typu fronty, použijte příkaz **createWMQQueue** .
- Chcete-li vytvořit místo určení typu tématu, použijte příkaz **createWMQTopic** .

Chcete-li upravit prostředek produktu JMS pro poskytovatele systému zpráv produktu IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li upravit specifikaci aktivace, použijte příkaz **modifyWMQActivationSpec** .

  Typ specifikace aktivace nelze změnit. Například, nemůžete vytvořit specifikaci aktivace, do které zadáte všechny informace o konfiguraci ručně, a pak ji upravit tak, aby používala tabulku CCDT.
- Chcete-li upravit továrnu připojení, použijte příkaz **modifyWMQConnectionFactory** .
- Chcete-li upravit místo určení typu fronty, použijte příkaz **modifyWMQQueue** .
- Chcete-li upravit místo určení typu tématu, použijte příkaz **modifyWMQTopic** .

Chcete-li odstranit prostředek produktu JMS pro poskytovatele systému zpráv produktu IBM MQ ve specifickém oboru, použijte následující příkazy.

- Chcete-li odstranit specifikaci aktivace, použijte příkaz **deleteWMQActivationSpec** .
- Chcete-li odstranit továrnu připojení, použijte příkaz **deleteWMQConnectionFactory** .
- Chcete-li odstranit cíl typu fronty, použijte příkaz **deleteWMQQueue** .
- Chcete-li odstranit místo určení typu tématu, použijte příkaz **deleteWMQTopic** .

Chcete-li zobrazit informace o specifickém prostředku poskytovatele systému zpráv produktu IBM MQ , použijte následující příkazy.

- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k určité specifikaci aktivace, použijte příkaz **showWMQActivationSpec** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k určité faktorii připojení, použijte příkaz **showWMQConnectionFactory** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k určitému místu určení typu fronty, použijte příkaz **showWMQQueue** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty přidružené k místu určení typu tématu, použijte příkaz **deleteWMQTopic** .

Chcete-li spravovat nastavení pro adaptér prostředků produktu IBM MQ nebo pro poskytovatele systému zpráv produktu IBM MQ , použijte následující příkazy.

- Chcete-li spravovat nastavení adaptéru prostředků produktu IBM MQ , který je instalován v určitém oboru, použijte příkaz **manageWMQ** .
- Chcete-li zobrazit všechny parametry a jejich hodnoty, které lze nastavit pomocí příkazu **manageWMQ** , použijte příkaz **showWMQ** . Tato nastavení se vztahují buď k adaptéru prostředků produktu IBM MQ , nebo k poskytovateli systému zpráv produktu IBM MQ . Příkaz **showWMQ** také zobrazuje všechny přizpůsobené vlastnosti, které jsou nastaveny na adaptéru prostředků IBM MQ .

Související pojmy

“Správci front s více instancemi” na stránce 457
Správci front s více instancemi jsou instance stejného správce front konfigurovaného na různých serverech. Jedna instance správce front je definována jako aktivní instance a jiná instance je definována jako instance v pohotovostním režimu. Dojde-li k selhání aktivní instance, správce front s více instancemi se automaticky restartuje na záložním serveru.

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 381
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

Použití sdílených odběrů produktu JMS 2.0

V produktu WebSphere Application Server traditional 9.0můžete konfigurovat a používat sdílené odběry JMS 2.0 s produktem IBM MQ 9.0.

Informace o této úloze

Specifikace JMS 2.0 zavedla koncepci sdílených odběrů, které umožňují otevření jednoho odběru jedním nebo více spotřebiteli. Tyto zprávy jsou sdíleny mezi všemi těmito spotřebiteli. Neexistuje žádné omezení, pokud jsou tito spotřebitelé příliš dlouho, dokud se připojují ke stejnému správci front.

Sdílené odběry mohou být buď trvalé, nebo netrvalé, se stejnou sémantikou jako to, na které se nyní odkazuje jako na nesdílené odběry.

Aby byl spotřebitel schopen identifikovat odběr, který má být použit, je třeba zadat název odběru. Tento proces je podobný nesdíleným trvalým odběrům, ale je vyžadován název odběru ve všech případech, kdy je vyžadován sdílený odběr. Hodnota clientIDse však v případě trvalého sdíleného-subscription; nepožaduje, ale není povinná.

Zatímco sdílené odběry lze považovat za mechanizmus vyrovnávání zátěže, a to ani v IBM MQ , ani ve specifikaci JMS 2.0 neexistuje závazek, jak se zprávy distribuují mezi spotřebiteli.

V produktu WebSphere Application Server traditional 9.0 je předinstalovaný adaptér prostředků produktu IBM MQ 9.0 .

Následující kroky ukazují, jak nakonfigurovat specifikaci aktivace pro použití sdíleného trvalého nebo sdíleného trvalého odběru pomocí administrativní konzoly serveru WebSphere Application Server traditional .

Postup

Nejprve vytvořte objekty v produktu JNDI.

1. Vytvořte místo určení tématu v produktu JNDI jako normální (viz “Konfigurace prostředků produktu JMS pomocí administrativní konzoly” na stránce 626).
2. Vytvořte specifikaci aktivace (viz “Konfigurace prostředků produktu JMS pomocí administrativní konzoly” na stránce 626).

   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 jiný než trvalý odběr, nemůžete v tomto bodě zadat název. Místo toho je třeba vytvořit přizpůsobenou vlastnost pro název odběru.

Aktualizujte specifikaci aktivace, kterou jste vytvořili, s požadovanými přizpůsobenými vlastnostmi. Existují dvě přizpůsobené vlastnosti, které možná budete muset uvést:

- Ve všech případech je třeba vytvořit přizpůsobenou vlastnost a určit, že tato specifikace aktivace by měla používat sdílený odběr.
- Pokud byl odběr vytvořen jako netrvalý, vlastnost názvu odběru musí být nastavena jako přizpůsobená vlastnost.

Následující tabulka zobrazuje platnou hodnotu, kterou lze zadat pro každou přizpůsobenou vlastnost:

Název vlastnosti	Typ	Platné hodnoty
sharedSubscription	Řetězec	true, false
subscriptionName	Řetězec	Řetězec jazyka Java bez nulové délky

3. Vyberte specifikaci aktivace ze seznamu zobrazeného ve formuláři **Kolekce specifikací aktivace** .

   Podrobnosti specifikace aktivace se zobrazí ve formuláři **Nastavení specifikace aktivace poskytovatele systému zpráv produktuIBM MQ** .
4. Na formuláři **Nastavení specifikace aktivace poskytovatele systému zpráv produktuIBM MQ** 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 poté zadejte následující podrobnosti:

   Název

   Název přizpůsobené vlastnosti, která je v tomto případě `subscriptionName`.

   Hodnota

   Hodnota přizpůsobené vlastnosti. Názvy JNDI byste mohli použít 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 poté zadejte následující podrobnosti:

   Název

   Název přizpůsobené vlastnosti, která je v tomto případě `sharedSubscription`.

   Hodnota

   Hodnota přizpůsobené vlastnosti. Chcete-li určit, že specifikace aktivace používá sdílený odběr, nastavte hodnotu na hodnotu `true`. Budete-li později chtít přestat používat sdílený odběr pro tuto specifikaci aktivace, můžete toto provést nastavením hodnoty 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. Když jsou vlastnosti nastaveny, restartujte aplikační server.

   Objekty typu message-driven bean (MDB) pro specifikace aktivace jsou poté řízeny při přijetí zpráv, ale pouze objekty MDB sdílejí odeslané zprávy.

Související pojmy

Klonované a sdílené odběry

Trvalost odběru

Související úlohy

Konfigurace adaptéru prostředků pro příchozí komunikaci

Související informace pro WebSphere Application Server traditional 9.0

Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ

Specifikace aktivace poskytovatele systému zpráv produktu IBM MQ

Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ

Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ
Konfigurace přizpůsobených vlastností pro prostředky JMS poskytovatele systému zpráv IBM MQ

Použití vlastností JMS 2.0 ConnectionFactory a Destination Lookup

V produktu WebSphere Application Server traditional 9.0lze vlastnosti ConnectionFactoryLookup a DestinationLookup specifikace aktivace poskytnout s názvem JNDI spravovaného objektu, který má být použit v předvolbách pro další vlastnosti specifikace aktivace.

Informace o této úloze

Specifikace JMS 2.0 určuje ve specifikaci aktivace dvě další vlastnosti použité k řízení zpráv objektů typu message-driven bean (MDB). Dříve musel každý dodavatel v rámci specifikace aktivace zadat přizpůsobené vlastnosti, aby poskytl podrobnosti vyžadované pro připojení k systému zpráv a definování místa určení, ze kterého mají být zprávy získaní.

Nyní lze použít standardní vlastnosti connectionFactoryLookup a destinationLookup k poskytnutí názvu JNDI relevantního objektu k vyhledání a použití. V produktu WebSphere Application Server traditional 9.0 je předinstalovaný adaptér prostředků produktu IBM MQ 9.0 .

Následující kroky ukazují, jak upravit a použít tyto dvě vlastnosti pomocí administrativní konzoly produktu WebSphere Application Server traditional .

Postup

Nejprve vytvořte objekty v produktu JNDI.

1. Vytvořte ConnectionFactory v JNDI jako normální (viz “Konfigurace prostředků produktu JMS pomocí administrativní konzoly” na stránce 626).
2. Vytvořte cíl v JNDI jako normální (viz “Konfigurace prostředků produktu JMS pomocí administrativní konzoly” na stránce 626).

   Cílový objekt musí mít správné hodnoty.
3. Vytvořte specifikaci aktivace s použitím všech potřebných hodnot (viz “Konfigurace prostředků produktu JMS pomocí administrativní konzoly” na stránce 626).

   Specifikaci aktivace můžete vytvořit přesně s vlastnostmi, které potřebujete. Měli byste však mít na paměti následující pokyny:

   - Chcete-li, aby adaptér prostředků produktu IBM MQ používal továrnu připojení produktu Java EE a vlastnosti vyhledávání místa určení, je méně relevantní, jaké vlastnosti se používají při vytváření specifikace aktivace (viz VlastnostiActivationSpec ConnectionFactorya vlastnosti DestinationLookup.
   - Nicméně jakákoli vlastnost, která ještě není definována v továrně připojení nebo v cíli, musí být stále uvedena ve specifikaci aktivace. Proto musíte definovat vlastnosti odběratele připojení a další vlastnosti a informace o ověření, které se používají při vytvoření připojení.
   - Z vlastností, které jsou definovány na faktorii připojení, má vlastnost ClientID speciální zpracování. Důvodem je skutečnost, že běžný scénář používá jednu továrnu připojení s více specifikacemi aktivace. To zjednodušuje administraci, avšak specifikace produktu JMS vyžaduje jedinečné ID klientů, a proto specifikace aktivace potřebuje mít schopnost přepsat jakoukoli hodnotu nastavenou na ConnectionFactory. Pokud není ve specifikaci aktivace nastavena žádná hodnota ClientID , použije se žádná hodnota z továrny připojení.

Buď aktualizujte specifikaci aktivace, kterou jste vytvořili se dvěma novými přizpůsobenými vlastnostmi, pomocí administrativní konzoly produktu WebSphere Application Server , jak je popsáno v kroku “4” na stránce 633, nebo použijte anotace místo toho, jak je popsáno v kroku “5” na stránce 634.

4. Aktualizujte specifikaci aktivace v administrativní konzole produktu WebSphere Application Server .

   Tyto dvě vlastnosti musí být nastaveny na panelu přizpůsobených vlastností specifikace aktivace. Tyto vlastnosti nejsou přítomny v hlavním panelu specifikace aktivace nebo v průvodci vytvořením aktivační specifikace.

   a) Vyberte specifikaci aktivace ze seznamu zobrazeného ve formuláři **Kolekce specifikací aktivace** .

Podrobnosti specifikace aktivace se zobrazí ve formuláři **Nastavení specifikace aktivace poskytovatele systému zpráv produktuIBM MQ** .

b) Na formuláři **Nastavení specifikace aktivace poskytovatele systému zpráv produktuIBM MQ** klepněte na volbu **Přizpůsobené vlastnosti**.

Zobrazí se formulář **Přizpůsobené vlastnosti** .

c) Na formuláři **Přizpůsobené vlastnosti** vytvořte dvě nové přizpůsobené vlastnosti typu java.lang.String.

V každém případě klepněte na volbu **Nový** a poté zadejte následující podrobnosti pro přizpůsobenou vlastnost:

Název

Název přizpůsobené vlastnosti, buď `connectionFactoryLookup` , nebo `destinationLookup`.

Hodnota

Hodnota přizpůsobené vlastnosti. Názvy JNDI byste mohli použít 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 bude nyní tyto hodnoty používat k vytvoření továrny připojení a místa určení. Při implementaci objektu typu message-driven bean neexistuje žádný požadavek na nastavení konfigurace hodnoty produktu JNDI .

5. Používejte anotace místo specifikace aktivace.

Je také možné použít anotace v kódu objektu MDB k určení hodnot. Například při použití názvů JNDI `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 sjednocené továrny připojení pro poskytovatele systému zpráv produktu IBM MQ

Konfigurace tématu pro poskytovatele systému zpráv produktu IBM MQ

Specifikace aktivace poskytovatele systému zpráv produktu IBM MQ

Vytvoření specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ

Konfigurace specifikace aktivace pro poskytovatele systému zpráv produktu IBM MQ

Konfigurace přizpůsobených vlastností pro prostředky JMS poskytovatele systému zpráv IBM MQ

Konfigurace aplikačního serveru pro použití nejnovější úrovně údržby adaptéru prostředků

Chcete-li zajistit automatickou aktualizaci adaptéru prostředků produktu IBM MQ na nejnovější dostupnou úroveň údržby při použití opravných sad produktu WebSphere Application Server , můžete nakonfigurovat všechny servery ve svém prostředí tak, aby používaly nejnovější verzi adaptéru prostředků obsaženou v sadě oprav produktu WebSphere Application Server , kterou jste použili při instalaci jednotlivých uzlů.

Než začnete

Důležité: Používáte-li produkt WebSphere Application Server 8.5 nebo starší na libovolné platformě, neinstalujte adaptér prostředků produktu IBM MQ 8.0 nebo novější na aplikační server. Adaptér prostředků produktu IBM MQ 8.0 nebo novější může být implementován pouze na aplikační server, který podporuje produkt JMS 2.0. Avšak produkt WebSphere Application Server 8.5 nebo starší podporuje pouze JMS 1.1. Tyto verze produktu WebSphere Application Server jsou dodávány s adaptérem prostředků produktu IBM WebSphere MQ 7.0 , který lze použít k připojení ke správci front produktu IBM MQ 8.0 pomocí přenosu BINDINGS nebo CLIENT.

Informace o této úloze

Tuto úlohu použijte, pokud se na vaši konfiguraci vztahuje kterákoliv z následujících okolností a vy chcete nakonfigurovat všechny servery ve vašem prostředí pro použití nejnovější verze adaptéru prostředků IBM MQ :

- Protokoly prostředí JVM libovolného aplikačního serveru ve vašem prostředí zobrazí po použití produktu WebSphere Application Server 7.0 opravné sady 1 nebo novější následující informace o verzi adaptéru prostředků produktu IBM MQ :

  ```
  Verze implementace WMSG1703I:RAR 7.0.0.0-k700-L080820
  ```

- Protokoly JVM všech aplikačních serverů ve vašem prostředí obsahují následující položku:

  ```
  WMSG1625E: Nebylo možné zjistit
  Kód poskytovatele systému zpráv produktu IBM MQ na zadané cestě < null>
  ```

- Jeden nebo více uzlů bylo dříve ručně aktualizováno tak, aby používalo specifickou úroveň údržby adaptéru prostředků produktu IBM MQ , který je nyní nahrazený nejnovější verzí adaptéru prostředků obsaženého v aktuální úrovni údržby produktu WebSphere Application Server .

Adresář *profile_root* , na který se příklady odkazují, je domovským adresářem profilu produktu WebSphere Application Server , například `C:\Program Files\IBM\WebSphere\AppServer1`.

Po provedení následujících kroků pro všechny buňky a instalace jediného serveru ve vašem prostředí budou servery při použití nové opravné sady produktu WebSphere Application Server automaticky přijímat údržbu adaptéru prostředků produktu IBM MQ .

Postup

1. Spusťte aplikační server. Je-li 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 produktu IBM MQ .
   a) Otevřete okno příkazového řádku a přejděte do adresáře *profile_root*`\bin` .

      Zadejte například `cd C:\Program Files\IBM\WebSphere\AppServer1\bin`.

   b) Spusťte nástroj wsadmin tak, že zadáte příkaz `wsadmin.bat -lang jython`, a pak, pokud jste k tomu vyzváni, zadejte své jméno uživatele a heslo.

   c) Napište následující příkaz a pak dvakrát klávesu Return:

```
wmqInfoMBeansUnsplit = AdminControl.queryNames("WebSphere:type=WMQInfo,*")
wmqInfoMBeansSplit = AdminUtilities.convertToList(wmqInfoMBeansUnsplit)
for wmqInfoMBean in wmqInfoMBeansSplit: print wmqInfoMBean; print AdminControl.invoke(wmqInfoMBean,
'getInfo', '')
```

      Tento příkaz můžete také spustit v jazyce Jacl. Další informace o tom, jak to provést, najdete v tématu *Zajištění toho, aby servery používaly nejnovější dostupnou úroveň údržby adaptéru prostředků produktu IBM MQ* v dokumentaci produktu WebSphere Application Server .

   d) Najděte zprávu `WMSG1703I` ve zobrazeném výstupu z příkazu a zkontrolujte úroveň adaptéru prostředků.

      Například pro WebSphere Application Server 7.0.1 Fix Pack 5 by zpráva měla být:

      ```
      WMSG1703I: Verze implementace RAR 7.0.1.3-k701-103-100812
      ```

Tato zpráva zobrazuje, že verze je 7.0.1.3-k701-103-100812, což je správná úroveň adaptéru prostředků pro tuto opravnou sadu. Pokud se však místo toho zobrazí následující zpráva, znamená to, že je třeba upravit adaptér prostředků na správnou úroveň údržby pro opravnou sadu 15.

```
WMSG1703I: 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 IBM MQ Resource Adapter") or (desc == "WAS 7.0.0.1 Built In IBM MQ
Resource Adapter"):
    print "Updating archivePath and classpath of " + ra
    AdminConfig.modify(ra, [['archivePath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar"]])
    AdminConfig.unsetAttributes(ra, ['classpath'])
    AdminConfig.modify(ra, [['classpath', "${WAS_INSTALL_ROOT}/installedConnectors/wmq.jmsra.rar"]])
    AdminConfig.save()
  #end if
#end for
```

Tip: Při ukládání souboru se ujistěte, že je soubor uložen jako soubor python, nikoli jako textový soubor.

4. Use the WebSphere Application Server wsadmin tool to run the Jython script that you have just created.

   Otevřete příkazový řádek a přejděte do adresáře `\bin` v domovském adresáři pro WebSphere Application Server, například adresář `C:\Program Files\IBM\WebSphere\AppServer1\bin` , poté zadejte následující příkaz a stiskněte klávesu Return:

   ```
   wsadmin -lang jython -f convertWMQRA.py
   ```

   Pokud k tomu budete vyzváni, zadejte své jméno uživatele a heslo.

   Poznámka: Spustíte-li skript pro profil, který je součástí konfigurace síťové implementace, skript aktualizuje všechny profily, které v této konfiguraci potřebují aktualizaci. Úplná resynchronizace může být nutná, pokud již existují nekonzistence konfiguračního souboru.
5. Pracujete-li v konfiguraci síťové implementace, ujistěte se, že jsou agenti uzlů plně resynchronizovaní. Další informace naleznete v tématu Synchronizace uzlů pomocí skriptovacího nástroje wsadmin nebo Přidání, správa a odebrání uzlů.
6. Zastavte všechny servery v profilu. Je-li profil součástí konfigurace síťové implementace, zastavte také všechny členy klastru v konfiguraci, zastavte všechny agenty uzlu v konfiguraci a zastavte správce implementace. Pokud profil obsahuje administrativního agenta, zastavte administrativního agenta.
7. Spusťte příkaz **osgiCfgInit** z adresáře *profile_root*`/bin` .

   Příkaz `osgiCfgInit` resetuje mezipaměť třídy používanou běhovým prostředím OSGi. Je-li profil součástí konfigurace síťové implementace, spusťte příkaz **osgiCfgInit** z adresáře `profile_root/bin` každého profilu, který je součástí konfigurace.
8. Restartujte všechny servery v profilu. Je-li profil součástí konfigurace síťové implementace, můžete také restartovat všechny členy klastru v konfiguraci, restartovat všechny agenty uzlů v konfiguraci a restartovat správce implementace. Pokud profil obsahuje administrativního agenta, restartujte administrativního agenta.
9. Zopakujte krok 2 a zkontrolujte, zda je adaptér prostředků nyní na správné úrovni.

Jak pokračovat dále

Budete-li po provedení kroků popsaných v tomto tématu i nadále docházet k problémům a dříve jste použili tlačítko **Aktualizovat adaptér prostředků** na panelu Nastavení poskytovatele serveru JMS v administrativní konzole serveru WebSphere Application Server , abyste aktualizovali adaptér prostředků produktu IBM MQ na všech uzlech ve vašem prostředí, je možné, že se vyskytl problém popsaný v tématu APAR PM10308.

Související úlohy

Použití adaptéru prostředků produktu IBM MQ

Související informace pro WebSphere Application Server 8.5.5

Zajištění toho, aby servery používaly nejnovější dostupnou úroveň údržby adaptéru prostředků produktu IBM MQ

Synchronizace uzlů pomocí skriptovacího nástroje wsadmin

Přidání, správa a odebírání uzlů

Nastavení poskytovatele služeb JMS

Konfigurace vlastnosti produktu JMS PROVIDERVERSION

Poskytovatel systému zpráv produktu IBM MQ má tři režimy provozu: normální režim, normální režim s omezeními a režim migrace. Můžete nastavit vlastnost JMS **PROVIDERVERSION** , abyste vybrali, který z těchto režimů používá aplikace JMS k publikování a odběru.

Informace o této úloze

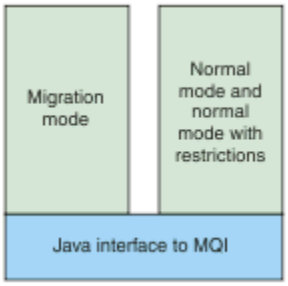
Výběr způsobu operace poskytovatele systému zpráv produktu IBM MQ lze primárně řídit nastavením vlastnosti továrny připojení PROVIDERVERSION. Režim operace může být také vybrán automaticky, pokud režim nebyl zadán.

Vlastnost **PROVIDERVERSION** rozlišuje mezi třemi režimy poskytovatele systému zpráv produktu IBM MQ :

Normální režim poskytovatele systému zpráv produktu IBM MQ
Normální režim používá všechny funkce správce front IBM MQ k implementaci služby JMS. Tento režim je optimalizovaný pro použití rozhraní API a funkčnosti JMS 2.0.

IBM MQ s omezeními
Normální režim s omezeními používá rozhraní API produktu JMS 2.0 , ale ne nové funkce, tj. sdílené odběry, odložené doručení a asynchronní odeslání.

Režim migrace poskytovatele systému zpráv produktu IBM MQ
Pomocí režimu migrace se můžete připojit ke správci front produktu IBM MQ 8.0 nebo novější, ale nejsou použity žádné funkce správce front produktu IBM WebSphere MQ 7.0 nebo novější, jako je například dopředné čtení a kontinuální načítání.



Obrázek 91. Režimy poskytovatele systému zpráv

Procedura

Chcete-li konfigurovat vlastnost **PROVIDERVERSION** pro specifickou továrnu připojení, postupujte takto:

- Chcete-li nakonfigurovat vlastnost produktu **PROVIDERVERSION** pomocí produktu IBM MQ Explorer, viz téma Konfigurace správců front a objektů.
- Chcete-li nakonfigurovat vlastnost **PROVIDERVERSION** pomocí administračního nástroje produktu JMS , přečtěte si téma Konfigurace správců front a objektů.

- Chcete-li nakonfigurovat vlastnost **PROVIDERVERSION** v aplikaci JMS pomocí rozšíření produktu IBM JMS nebo rozšíření IBM MQ JMS , prostudujte si témaVytvoření a konfigurace továren připojení a cílů v aplikaci IBM MQ classes for JMS.

Chcete-li potlačit nastavení režimu poskytovatele továrny připojení pro všechny továrny připojení v prostředí JVM, postupujte takto:

- Chcete-li potlačit nastavení režimu poskytovatele továrny připojení, použijte vlastnost `com.ibm.msg.client.wmq.overrideProviderVersion` .

  Pokud nemůžete změnit 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

Vlastnosti továrny připojení

Související úlohy

Odstraňování problémů s verzí poskytovatele JMS

Související odkazy

PROVIDERVERSION

Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

Režimy poskytovatele systému zpráv produktu IBM MQ

Můžete vybrat, který režim poskytovatele systému zpráv produktu IBM MQ bude aplikace JMS používat k publikování a odběru nastavením vlastnosti PROVIDERVERSION pro továrnu připojení na příslušnou hodnotu. V některých případech je vlastnost PROVIDERVERSION nastavena jako nespecifikovaná, v takovém případě klient JMS používá algoritmus k určení, jaký režim operace použít.

PROVIDERVERSION Hodnoty vlastností

Vlastnost továrny připojení **PROVIDERVERSION** můžete nastavit na některou z následujících hodnot:

8 - Normální režim
Aplikace JMS používá normální režim. Tento režim používá všechny funkce správce front produktu IBM MQ k implementaci produktu JMS.

7 - Normální režim s omezeními
Aplikace JMS používá normální režim s omezeními. Tento režim používá rozhraní JMS 2.0 API, ale ne nové funkce, jako sdílení odběrů, odložené doručení nebo asynchronní odeslání.

6 - Režim migrace
Aplikace JMS používá režim migrace. V režimu migrace používá produkt IBM MQ classes for JMS funkce a algoritmy podobné těm, které jsou dodávány s produktem IBM WebSphere MQ 6.0.

neurčeno (výchozí hodnota)
Klient JMS používá algoritmus k určení, který režim operace se používá.

Vámi zadaná hodnota ve vlastnosti **PROVIDERVERSION** musí být řetězec. Pokud zadáte volbu 8, 7 nebo 6, můžete to provést v některém z následujících formátů:

- V.R.M.F
- V.R.M
- V.R
- V

kde V, R, M a F jsou celá čísla větší nebo rovná nule. Hodnoty R, M a F jsou nepovinné a můžete je použít k upřesnění v případě potřeby řízení s vysokou úrovní granularity. Chcete-li například použít úroveň **PROVIDERVERSION** z 7, můžete nastavit **PROVIDERVERSION** = 7, `7.0`, `7.0.0` nebo `7.0.0.0`.

Typy objektů továrny připojení

Vlastnost **PROVIDERVERSION** lze nastavit pro následující typy objektů továrny připojení:

- MQConnectionFactory
- Továrna MQQueueConnection
- Továrna MQTopicConnection
- MQXAConnectionFactory
- Továrna MQXAQueueConnection
- Továrna MQXAQueueConnection
- Továrna MQXAQueueConnection
- Továrna MQXATopicConnection

Další informace o těchto různých typech továrny připojení najdete v tématu “Konfigurace objektů produktu JMS pomocí nástroje pro administraci” na stránce 616.

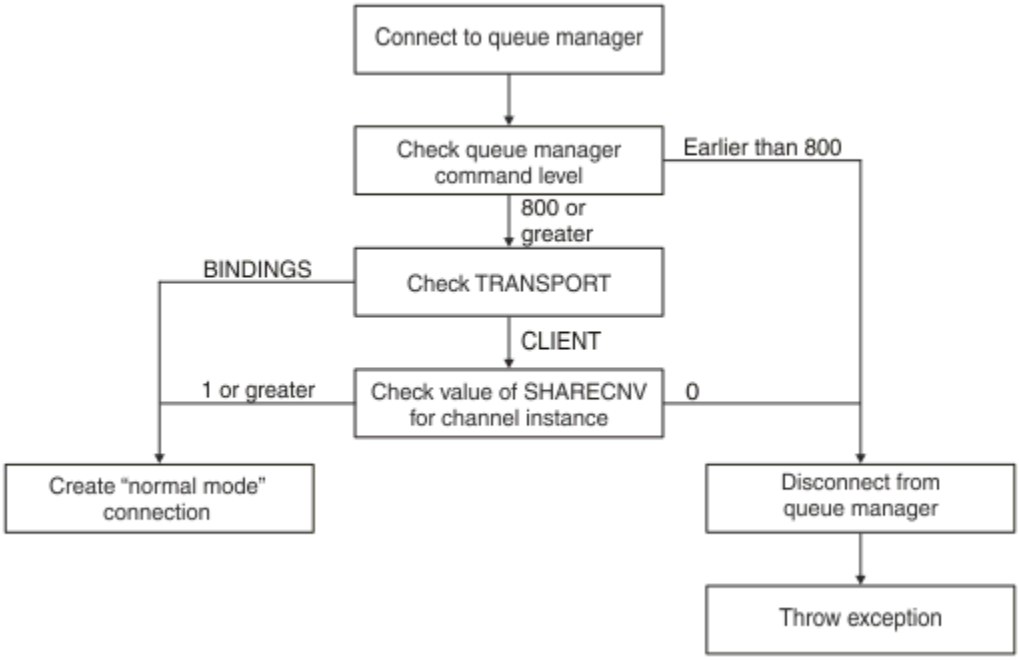
Související pojmy

Poskytovatel systému zpráv IBM MQ

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 k určení, zda lze vytvořit normální připojení režimu.



Obrázek 92. Normální režim PROVIDERVERSION

Je-li správce front určený v nastavení továrny připojení nastaven na úroveň 800 nebo vyšší a vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS, bude vytvořeno normální připojení režimu bez kontroly dalších vlastností.

Pokud má správce front uvedený v nastavení továrny připojení úroveň příkazů 800 nebo vyšší a vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, bude zkontrolována také vlastnost **SHARECNV** na kanálu připojení serveru. Tato kontrola je nutná, protože poskytovatel systému zpráv produktu IBM MQ v normálním režimu používá funkci sdílení konverzací. Proto je pro pokus o připojení normálního režimu

úspěšný pokus o vlastnost **SHARECNV** , která určuje počet konverzací, které lze sdílet, musí mít hodnotu 1 nebo vyšší.

Jsou-li všechny kontroly zobrazené ve vývojovém diagramu úspěšné, je možné použít normální připojení režimu ke správci front a všechny funkce rozhraní API a funkce produktu JMS 2.0 , tj. asynchronní odeslání, odložené doručení a sdílené předplatné.

Pokus o vytvoření připojení v normálním režimu selhává z následujících příčin:

- Správce front uvedený v nastavení továrny připojení má úroveň příkazů, která je starší než 800. V tomto případě metoda `createConnection` selže s výjimkou `JMSFMQ0003`.
- Vlastnost **SHARECNV** na kanálu připojení serveru je nastavena na hodnotu `0`. Pokud tato vlastnost nemá hodnotu 1 nebo vyšší, metoda `createConnection` selže s výjimkou `JMSCC5007`.

Související informace

Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

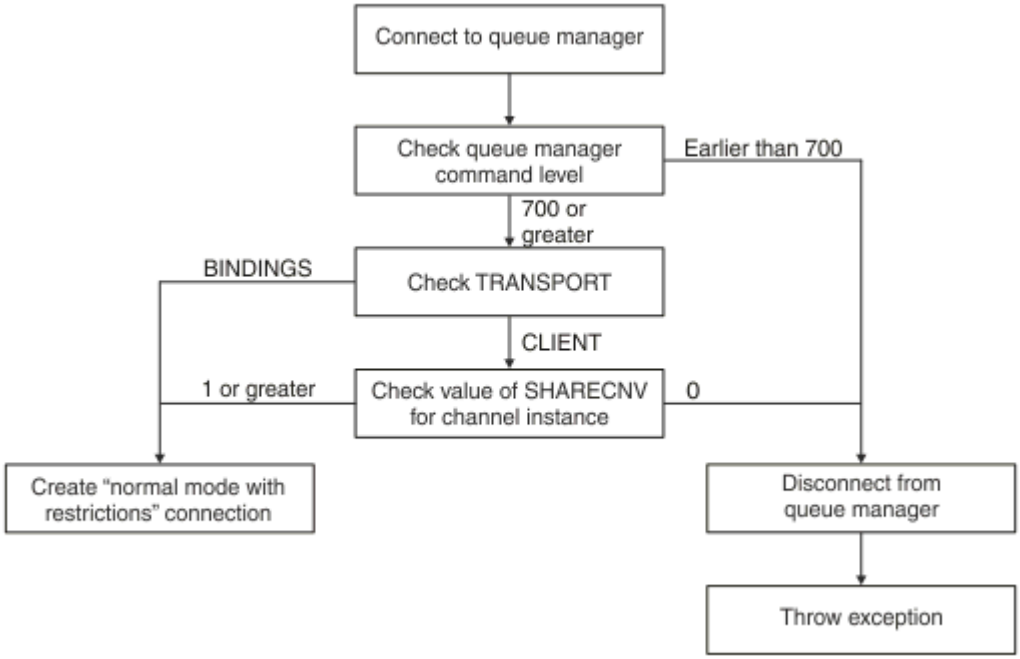
DEFINE CHANNEL (vlastnost SHARECNV)

TRANSPORT

Normální režim PROVIDERVERSION s omezeními

Normální režim s omezeními používá rozhraní API produktu JMS 2.0 , ale ne nové funkce produktu IBM MQ 8.0 nebo novější, jako např. sdílené odběry, odložené doručení nebo asynchronní odeslání.

Následující graf toku zobrazuje kontroly, které klient JMS provádí k určení, zda lze vytvořit normální režim s omezením připojení.



Obrázek 93. Normální režim PROVIDERVERSION s omezeními

Je-li správce front zadaný v nastavení továrny připojení nastaven na hodnotu 700 nebo vyšší a vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS, bude vytvořeno připojení v normálním režimu bez kontroly dalších vlastností.

Má-li správce front zadaný v nastavení faktorie připojení úroveň příkazu 700 nebo vyšší a vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, bude zkontrolována také vlastnost **SHARECNV** na kanálu připojení serveru. Tato kontrola je nutná, protože poskytovatel systému zpráv produktu IBM MQ v normálním režimu s omezeními používá funkci sdílení konverzací. Proto musí mít vlastnost **SHARECNV** , která řídí počet konverzací, které lze sdílet, hodnotu 1 nebo větší, pro normální režim s pokusem o omezení připojení.

Pokud jsou všechny kontroly zobrazené ve vývojovém diagramu úspěšné, vytvoří se normální režim s omezením připojení ke správci front a vy pak můžete použít rozhraní API produktu JMS 2.0 , ale ne asynchronní odeslání, odložené doručení nebo sdílené funkce odběru.

Pokus o vytvoření normálního režimu s omezováním připojení selhává z následujících důvodů:

- Správce front uvedený v nastavení továrny připojení má úroveň příkazů, která je starší než 700. V tomto případě se metoda `createConnection` nezdaří s výjimkou `JMSFCC5008`.
- Vlastnost **SHARECNV** na kanálu připojení serveru je nastavena na hodnotu `0`. Pokud tato vlastnost nemá hodnotu `1` nebo vyšší, metoda `createConnection` selže s výjimkou `JMSCC5007`.

Související informace

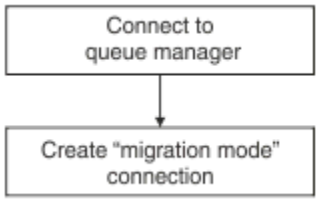
Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

DEFINE CHANNEL (vlastnost SHARECNV)

TRANSPORT

Režim migrace produktu PROVIDERVERSION

Pro režim migrace používá produkt IBM MQ classes for JMS funkce a algoritmy podobné těm, které jsou dodávány s produktem IBM WebSphere MQ 6.0, jako je publikování/odběr ve frontě, výběr implementovaný na straně klienta, nemultiplexové kanály a systém výzev používaný k implementaci listenerů.



Obrázek 94. Migrační režim PROVIDERVERSION

Chcete-li se připojit k produktu WebSphere Message Broker 6.0 nebo 6.1 pomocí produktu IBM MQ Enterprise Transport 6.0, musíte použít režim migrace.

Pomocí režimu migrace se můžete připojit ke správci front produktu IBM MQ 8.0 , ale žádná z nových funkcí správce front produktu IBM MQ classes for JMS se nepoužívá, například dopředné čtení nebo kontinuální načítání. Pokud máte klienta IBM MQ 8.0 nebo pozdější připojení k produktu IBM MQ 8.0 nebo novějším správci front na distribuované platformě, z/OS nebo správce front produktu IBM MQ 8.0 nebo novější v systému z/OS , pak je výběr zpráv proveden spíše správcem front než v systému klienta.

Je-li zadán režim migrace poskytovatele systému zpráv produktu IBM MQ a IBM MQ classes for JMS se pokusí použít některý z rozhraní API produktu JMS 2.0 , volání metody rozhraní API se nezdaří s výjimkou `JMSCC5007`.

Související informace

Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS

TRANSPORT

PROVIDERVERSION nespecifikováno

Není-li vlastnost **PROVIDERVERSION** továrny připojení určena, klient JMS používá algoritmus k určení, který režim operace se používá pro připojení ke správci front. Továrna připojení, která byla vytvořena v oboru názvů JNDI s předchozí verzí produktu IBM MQ classes for JMS , vezme neurčenou hodnotu, je-li továrna připojení použita s novou verzí produktu IBM MQ classes for JMS.

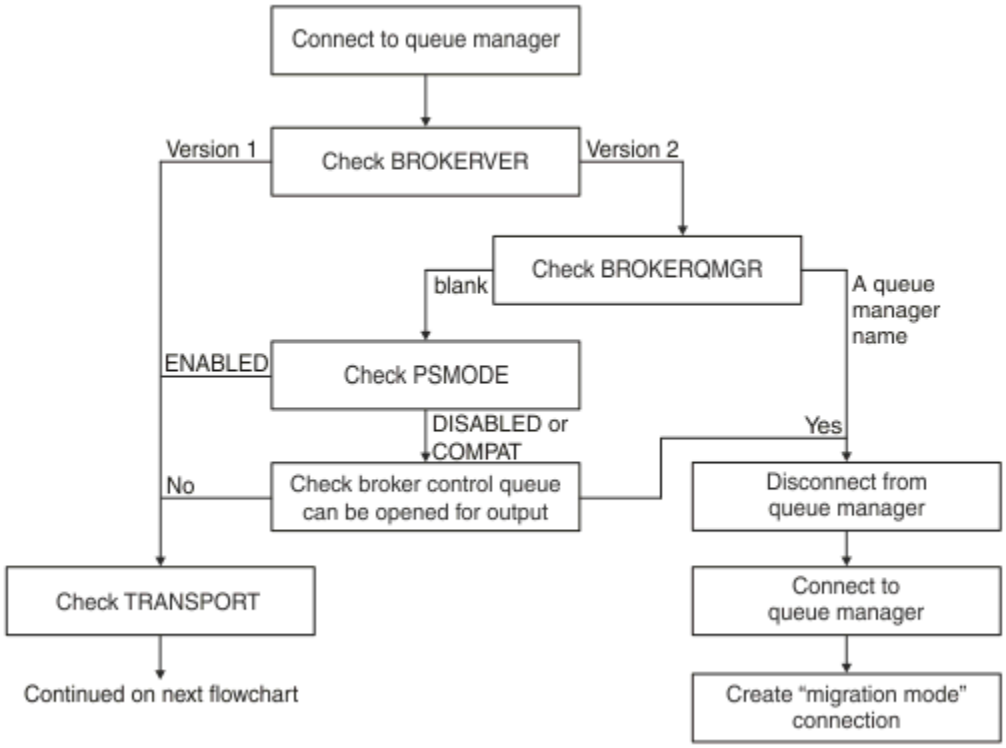
Není-li vlastnost **PROVIDERVERSION** určena, je algoritmus použit při volání metody `createConnection` . Algoritmus kontroluje určitý počet vlastností továrny připojení a určuje, zda je vyžadován normální režim poskytovatele systému zpráv produktu IBM MQ , normální režim s omezeními nebo režim migrace poskytovatele systému zpráv produktu IBM MQ . Normální režim se vždy nejprve pokusí o první režim a pak normální režim s omezeními. Pokud nelze vytvořit ani jeden z těchto typů

připojení, odpojí se klient JMS od správce front a potom se znovu připojí ke správci front, aby se pokusil o připojení v režimu migrace.

Kontrola vlastností produktů BROKERVER, BROKERQMGR, PSMODEa BROKERCONQ

Kontrola hodnot vlastností začíná vlastností **BROKERVER** , jak ukazuje Obrázek 1.

Je-li vlastnost **BROKERVER** nastavena na hodnotu V1, bude vlastnost **TRANSPORT** se zaškrtnutá jako další, jak ukazuje Obrázek 2. Je-li však vlastnost **BROKERVER** nastavena na hodnotu V2, další kontrola zobrazená na Obrázku 1 se provádí před kontrolou vlastnosti **TRANSPORT** .



Obrázek 95. PROVIDERVERZE není

Je-li vlastnost **BROKERVER** nastavena na hodnotu V2, musí být vlastnost **BROKERQMGR** pro normální připojení režimu `prázdná`. Kromě toho musí být atribut **PSMODE** ve správci front nastaven na hodnotu `ENABLED` nebo nesmí být otevřena řídicí fronta zprostředkovatele určená vlastností **BROKERCONQ** pro výstup.

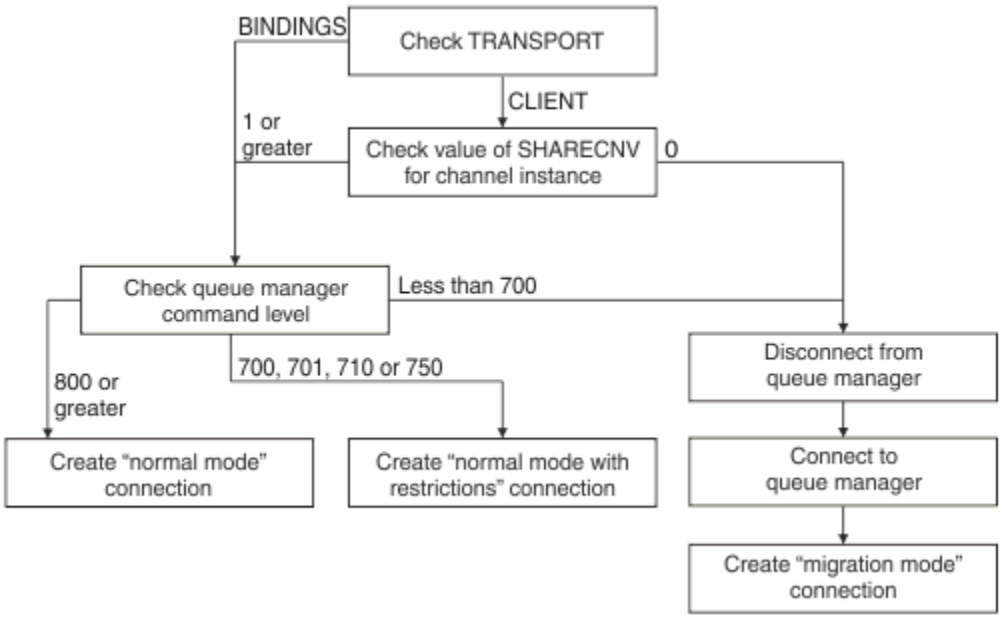
Jsou-li hodnoty vlastností nastaveny jako vyžadované pro normální připojení režimu, kontrola dalšího se přesune na vlastnost **TRANSPORT** , jak ukazuje Obrázek 2.

Nejsou-li hodnoty vlastností nastaveny jako vyžadované pro normální připojení režimu, klient JMS se odpojí od správce front a poté se znovu připojí a vytvoří připojení režimu migrace. K tomu dojde v následujících případech:

- Pokud je vlastnost **BROKERQMGR** `blank` a atribut **PSMODE** na správci front je nastaven na hodnotu `COMPAT` nebo `DISABLED` a fronta řízení zprostředkovatele zadaná vlastností **BROKERCONQ** může být otevřena pro výstup (to znamená, že výstup `MQOPEN` je úspěšný).
- Pokud vlastnost **BROKERQMGR** uvádí název fronty.

Kontrola vlastnosti TRANSPORT a úrovně příkazu

Obrázek 2 zobrazuje kontroly provedené pro vlastnost **TRANSPORT** a úroveň příkazů správce front.



Obrázek 96. PROVIDERVERSION nespecifikováno (pokračování)

Připojení normální režim je vytvořeno v jednom z následujících případů:

- Vlastnost **TRANSPORT** továrny připojení je nastavena na hodnotu BINDINGS a správce front má úroveň příkazů 800 nebo vyšší.
- Vlastnost **TRANSPORT** je nastavena na hodnotu CLIENT, vlastnost **SHARECNV** kanálu připojení k serveru má hodnotu 1 nebo vyšší a správce front má úroveň příkazů 800 nebo vyšší.

Má-li správce front úroveň příkazů 710 nebo 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** kanálu připojení serveru má hodnotu 0.

Související informace

Závislosti mezi vlastnostmi objektů produktu IBM MQ classes for JMS
ALTER QMGR (atribut PSMODE)
BROKERCONQ
BROKERQMGR
BROKERVER
DEFINE CHANNEL (vlastnost SHARECNV)
TRANSPORT

Kdy přepsat výchozí nastavení PROVIDERVERSION

Je-li továrna připojení vytvořená v oboru názvů JNDI s předchozí verzí produktu IBM MQ classes for JMS použita s novou verzí produktu IBM MQ classes for JMS, vlastnost **PROVIDERVERSION** pro továrnu připojení je nastavena na výchozí hodnotu `unspecified` a používá se k určení, který režim poskytovatele systému zpráv produktu IBM MQ se používá. Avšak existují dva případy, kdy musíte přepsat výchozí výběr pro vlastnost **PROVIDERVERSION** , aby mohl produkt IBM MQ classes for JMS pracovat správně.

Poznámka: Režim migrace, který je popsán v tomto tématu, je pro migraci z produktu IBM WebSphere MQ 6.0 do produktu IBM WebSphere MQ 7.0. Nevztahuje se na migraci z novějších vydání.

IBM WebSphere MQ 6.0, WebSphere Application Server 6.0.xa WebSphere Message Broker 6 jsou mimo podporu, a proto je toto téma zahrnuto pouze pro referenční účely.

Je-li vlastnost **PROVIDERVERSION** nastavena na výchozí hodnotu `unspecified`, algoritmus se používá k určení, jaký režim operace použít, jak je popsáno v "PROVIDERVERSION nespecifikováno" na stránce 641. Tento algoritmus však nelze použít v následujících dvou scénářích.

1. Pokud jsou WebSphere Message Broker a WebSphere Event Broker v režimu kompatibility, musíte zadat hodnotu pro vlastnost **PROVIDERVERSION** , aby WebSphere Message Broker a WebSphere Event Broker fungovaly správně.
2. Používáte-li WebSphere Application Server 6.0.1, WebSphere Application Server 6.0.2nebo WebSphere Application Server 6.1, továrny připojení jsou definovány pomocí administrativní konzoly serveru WebSphere Application Server .

   V produktu WebSphere Application Serverje výchozí hodnota vlastnosti **BROKERVER** v továrně připojení V2. Výchozí hodnota vlastnosti **BROKERVER** pro továrny připojení, které jsou vytvořeny pomocí nástroje pro administraci produktu JMS **JMSAdmin** nebo IBM MQ Explorer je V1. Tato vlastnost je nyní `nespecifikovaná` v produktu IBM MQ.

Pokud je vlastnost **BROKERVER** nastavena na hodnotu V2, protože byla vytvořena produktem WebSphere Application Server nebo byla použita továrna připojení pro publikování/odběr před a má existujícího správce front, který má definovanou vlastnost produktu **BROKERCONQ** (protože byla použita pro systém zpráv publikování/odběru), je použit režim migrace poskytovatele systému zpráv produktu IBM MQ .

Pokud však chcete, aby aplikace používala komunikaci typu P2P a aplikace používá existujícího správce front, který byl někdy použit pro publikování/odběr, a má továrnu připojení s hodnotou **BROKERVER** nastavenou na hodnotu 2, což je výchozí nastavení, pokud byla továrna připojení vytvořena v produktu WebSphere Application Server, bude použit režim migrace poskytovatele systému zpráv produktu IBM MQ . Použití režimu migrace poskytovatele systému zpráv produktu IBM MQ v tomto případě není nutné; místo toho použijte normální režim poskytovatele systému zpráv produktu IBM MQ . K práci můžete použít jednu z následujících metod:

- Nastavte **BROKERVER** na 1 nebo nespecifikované. Volba, kterou zvolíte, závisí na aplikaci.
- Nastavte **PROVIDERVERSION** na 8, nebo 7, což jsou přizpůsobené vlastnosti v produktu WebSphere Application Server 6.1.

  Případně můžete použít vlastnost konfigurace klienta nebo upravit připojení správce front tak, aby nepoužíval sadu vlastností **BROKERCONQ** , nebo tuto frontu nepoužívat.

Konfigurace informací o verzi poskytovatele v produktu WebSphere Application Server

Chcete-li konfigurovat informace o verzi poskytovatele v produktu WebSphere Application Server, můžete buď použít administrativní konzolu, nebo příkazy wsadmin.

Postup

Chcete-li konfigurovat informace o verzi poskytovatele pro továrnu připojení nebo objekt specifikace aktivace produktu IBM MQ v produktu WebSphere Application Server, viz *Související informace* , kde najdete odkazy na další informace v dokumentaci produktu WebSphere Application Server .

Související informace pro WebSphere Application Server 8.5.5

Nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ

`createWMQConnectionFactory` příkaz

Nastavení specifikace aktivace poskytovatele systému zpráv produktu IBM MQ

`createWMQActivationSpec` příkaz

Související informace pro WebSphere Application Server 8.0.0

Nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ

`createWMQConnectionFactory` příkaz

Nastavení specifikace aktivace produktu IBM MQ

`createWMQActivationSpec` příkaz

Související informace pro WebSphere Application Server 7.0.0
Nastavení továrny připojení poskytovatele systému zpráv produktu IBM MQ
createWMQConnectionFactory příkaz
Nastavení specifikace aktivace produktu IBM MQ
createWMQActivationSpec příkaz

Odebrání trvalých odběrů produktu WebSphere Application Server

Pokud použijete poskytovatele systému zpráv produktu IBM MQ s produkty WebSphere Application Server 7.0 a IBM MQ 8.0, nebudou odebrány trvalé odběry vytvořené aplikacemi typu message-driven bean, které jsou svázány se specifikacemi aktivace, a nikoli. Trvalé odběry lze odebrat buď pomocí obslužného programu příkazového řádku IBM MQ Explorer , nebo pomocí obslužného programu příkazového řádku IBM MQ .

Informace o této úloze

Aplikace typu message-driven bean, která odebere trvalý odběr, může být konfigurována tak, aby používala buď port modulu listener, nebo specifikaci aktivace, za předpokladu, že aplikace běží uvnitř instance produktu WebSphere Application Server 7.0 nebo IBM MQ 8.0 , která používá produkt Normální režim poskytovatele systému zpráv produktu IBM MQ k připojení k produktu IBM MQ.

Je-li aplikace objektu typu message-driven bean svázána s portem modulu listener, pak poskytovatel systému zpráv produktu IBM MQ vytvoří trvalý odběr aplikace při prvním spuštění aplikace. Trvalý odběr je odebrán při odinstalaci aplikace objektu typu message driven bean z aplikačního serveru a restartováním aplikačního serveru.

Aplikace typu message-driven bean, která je svázána se specifikací aktivace, pracuje mírně odlišným způsobem. Trvalý odběr je vytvořen pro aplikaci při prvním spuštění aplikace. Trvalý odběr však nebude odebrán při odinstalaci aplikace a restartování aplikačního serveru.

To může vést k řadě trvalých odběrů, které zbývají u stroje publikování/odběru IBM MQ pro aplikace, které již nejsou instalovány v systému WebSphere Application Server . Tyto odběry jsou známy jako "osiřelé odběry" a mohou vést k problémům ve správci front, je-li stroj publikování/odběru spuštěn.

Je-li zpráva publikována na téma, stroj publikování/odběru IBM MQ vytvoří kopii této zprávy pro každý trvalý odběr registrovaný v daném tématu a vloží jej do interní fronty. Aplikace, které používají tento trvalý odběr, budou poté vyzvednou a spotřebovávat zprávu z této interní fronty.

Pokud aplikace typu message-driven bean, která používala tento trvalý odběr, již není nainstalována, budou nadále prováděny kopie publikovaných zpráv pro danou aplikaci. Tyto zprávy však nebudou nikdy zpracovány, což znamená, že ve vnitřní frontě může být velký počet zpráv, které nebudou nikdy odebrány.

Než začnete

Odběry, které jsou registrovány s produktem IBM MQ Publish/Subscribe Engine, budou mít k sobě přidružené názvy odběru.

Trvalé odběry vytvořené poskytovatelem systému zpráv produktu WebSphere Application Server IBM MQ pro objekty bean řízené zprávami, 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 produktu IBM MQ , kde je spuštěn stroj publikování/odběru.

Identifikátor klienta
Jedná se o hodnotu vlastnosti ID klienta ve specifikaci aktivace, na kterou je objekt typu message-driven bean svázán.

Název odběru
Jedná se o hodnotu názvu odběru vlastnosti specifikace aktivace pro specifikaci aktivace, kterou byla konfigurována aplikace objektu typu message driven bean pro použití.

Předpokládejme například, že máme specifikaci aktivace, která byla nastavena pro připojení ke správci front testQM. Specifikace aktivace má nastavu následující vlastnosti:

- ID klienta = testClientID
- Název odběru = durableSubscription1

Je-li objekt typu message-driven bean, který trvá na trvalém odběru, svázán s touto specifikací aktivace, vytvoří se odběr na systému publikování/odběru IBM MQ na správci front testQM , který má následující název odběru:

- JMS:testQM:testClientID:durableSubscription1

Odběry, které byly registrovány s použitím stroje publikování/odběru produktu IBM MQ pro daného správce front, lze zobrazit jedním z následujících způsobů:

- První možností je použití Průzkumníka produktu MQ . Pokud byl program Průzkumník produktu MQ připojen ke správci front používanému k publikování/odběru, lze zobrazit seznam odběratelů, kteří jsou aktuálně registrováni u publikování/odběru stroje publikování, klepnutím na položku `IBM WebSphere MQ ->`*`queue manager name`*`-> Subscriptions` v navigačním podokně.
- Druhým způsobem, jak zobrazit odběry registrované pomocí stroje publikování/odběru, je použít obslužný program příkazového řádku IBM MQ **runmqsc** a spustit příkaz **display sub**. Chcete-li tak učinit, vyvolejte příkazovou řádku, přejděte do adresáře *`WebSphere MQ`*`\bin` a spusťte příkaz **runmqsc**zadáním následujícího příkazu:

  – `runmqsc` *`queue manager name`*

  Po spuštění obslužného programu **runmqsc** zadejte následující příkaz k vypsání všech trvalých odběrů, které jsou aktuálně registrovány ve stroji publikování/odběru, který je spuštěn ve správci front, k němuž se produkt **runmqsc** připojil:

  – `display sub(*) durable`

Chcete-li zkontrolovat, zda jsou trvalé odběry registrované s generátory publikování/odběru stále aktivní:

1. Generujte seznam trvalých odběrů, které byly registrovány s použitím stroje publikování/odběru.
2. Pro každý trvalý odběr:
   - Podívejte se na název odběru pro trvalého odběratele a poznamenejte si hodnotu *identifikátor klienta* a *název odběru* .
   - Podívejte se na systémy WebSphere Application Server , které se připojují k tomuto generátoru publikování/odběru. Zjistěte, zda existují nějaké definované specifikace aktivace, které mají vlastnost ID klienta, která odpovídá hodnotě *identifikátor klienta* a vlastnosti názvu odběru, která odpovídá hodnotě *název odběru*.
   - Pokud nejsou nalezeny žádné specifikace aktivace, které mají vlastnosti ID klienta a názvu odběru, které odpovídají polím *identifikátor klienta* a *název_odběru* v názvu odběru IBM MQ , pak neexistují specifikace aktivace používající tento trvalý odběr. Trvalý odběr lze odstranit.
   - Je-li definována specifikace aktivace, která odpovídá názvu trvalého odběru, bude provedena konečná kontrola, kterou je třeba provést, je-li k dispozici aplikace typu message-driven bean používající tuto specifikaci aktivace. Postupujte takto:
     – Poznamenejte si název JNDI pro specifikaci aktivace, která odebrala trvalý odběr, v němž se momentálně hledáte.
     – Otevřete podokno Konfigurace v administrativní konzole produktu WebSphere Application Server pro každou aplikaci typu message-driven bean, která byla nainstalována.
     – V podokně Konfigurace klepněte na odkaz na vazby modulu listener objektu typu message driven bean.

- Zobrazí se tabulka s informacemi o aplikaci objektu typu message driven bean. Je-li ve sloupci Vazby vybrán přepínač specifikace aktivace a v poli Název cílového prostředku JNDI je uveden název JNDI pro specifikaci aktivace, která odebrala trvalý odběr, je odběr nadále používán a nelze jej odstranit.
- Pokud nelze nalézt žádné aplikace typu message-driven bean, které používají specifikaci aktivace, lze trvalý odběr odstranit.

Postup

Jakmile je identifikován "osiřelý" trvalý odběr, lze jej odstranit buď pomocí obslužného programu IBM MQ Explorer , nebo pomocí obslužného programu příkazového řádku IBM MQ **runmqsc**.

Chcete-li odstranit "osiřelý" trvalý odběr pomocí produktu 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 správnost názvu odběru zobrazeného v okně s potvrzením a klepněte na tlačítko **Ano**.

Produkt IBM MQ Explorer nyní odstraní odběr ze stroje publikování/odběru a vyčistí všechny vnitřní prostředky, které jsou k němu přidruženy (jako jsou nezpracované zprávy publikované pro téma, na němž byl registrován trvalý odběr).

Chcete-li odstranit "osiřelý" trvalý odběr pomocí obslužného programu příkazového řádku IBM MQ **runmqsc**, musí být příkaz **delete sub** spuštěn:

1. Otevřít relaci příkazového řádku
2. Přejděte do adresáře *IBM MQ*\bin .
3. Zadejte následující příkaz ke spuštění produktu **runmqsc**:

```
runmqsc queue manager name
```

4. Po spuštění obslužného programu **runmqsc** zadejte:

```
delete sub(Subscription name)
```

kde *Název odběru* je název odběru trvalého odběru, který má podobu:

- JMS:*queue manager name*:*client identifier*:*subscription name*

Konfigurace produktu Managed File Transfer

Po instalaci můžete nakonfigurovat funkce produktu Managed File Transfer .

Řešení vysoké dostupnosti systému IBM MQ můžete využít ke zlepšení odolnosti konfigurace produktu Managed File Transfer . Pokud agenti používají replikované správce datových front (RQMs), musíte je nakonfigurovat, aby mohli používat funkci plovoucí adresy IP. To znamená, že agenti používají stejnou adresu IP ke komunikaci s každou ze tří instancí RDR, které momentálně běží a automaticky se znovu připojí k překonání selhání (viz Vysoká dostupnost RDQM a Vytvoření a odstranění plovoucí adresy IP). Pokud použijete řešení správce front s více instancemi, pak aplikace používají jinou adresu IP ke komunikaci s každou instancí, kterou obsluhuje opětovné navázání spojení s klientem při překonání selhání (viz Správci front s více instancemi a Připojení kanálu a klienta).

Související pojmy

Rady a tipy pro použití produktu Managed File Transfer

Související úlohy

Monitorování prostředků produktu MFT

Přizpůsobení MFT s uživatelskými procedurami

Konfigurace MQMFTCredentials.xml

zabezpečeníManaged File Transfer
Zadání programů pro spouštění s produktem MFT
odstraňování problémůManaged File Transfer
Správa serveruManaged File Transfer

Související odkazy

MFT příkazy
Soubor MFT`agent.properties`
Zotavení a restart MFT

Volby konfigurace produktu MFT na platformách Multiplatforms

Produkt Managed File Transfer poskytuje sadu souborů vlastností, které obsahují klíčové informace o vašem nastavení a které jsou vyžadovány pro provoz. 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 se používají jako výchozí parametry pro všechny příkazy Managed File Transfer , pokud jste explicitně neuvedli jinou hodnotu na příkazovém řádku.

Chcete-li změnit výchozí sadu voleb konfigurace, kterou používáte, můžete použít příkaz **fteChangeDefaultConfigurationOptions** . Chcete-li změnit sadu voleb konfigurace, které 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 tato hodnota nezměnila. 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 nakonfigurujete 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 *název_agenta* je adresář agenta. Kromě souboru `agent.properties` tento adresář obsahuje adresář `exits` , který je výchozím umístěním uživatelských procedur uživatelské procedury a různých souborů XML generovanými příkazy **fteCreateBridgeAgent** a **fteCreateCDAgent** . V adresáři `agents` v sadě voleb konfigurace může být více než jeden adresář agenta.

soubory vlastností

installation.properties
Soubor `installation.properties` určuje název vaší výchozí sady voleb konfigurace. Tento vstupní bod ukazuje Managed File Transfer na strukturovanou sadu adresářů a souborů vlastností, které obsahují konfiguraci, jež má být použita. Typicky je název sady voleb konfigurace názvem přidruženého koordinačního správce front. Další informace o souboru `installation.properties` naleznete v tématu Soubor MFT installation.properties.

coordination.properties
Soubor `coordination.properties` určuje podrobnosti o připojení ke koordinačnímu správci front. Vzhledem k tomu, že několik instalací produktu Managed File Transfer může sdílet stejný koordinační správce front, můžete použít symbolický odkaz na společný soubor `coordination.properties` na sdílené jednotce. Další informace o souboru `coordination.properties` naleznete v souboru The MFT coordination.properties.

command.properties
Soubor MFT command.properties určuje správce front příkazů, k němuž se má připojit, když zadáte příkazy a informace, které produkt Managed File Transfer vyžaduje ke kontaktování tohoto správce front. Další informace o souboru `command.properties` naleznete v tématu 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` naleznete v tématu Soubor MFT `agent.properties`.

logger.properties
Soubor `logger.properties` určuje vlastnosti konfigurace pro moduly protokolování. Další informace o souboru `logger.properties` naleznete v tématu Vlastnosti konfigurace modulu protokolování produktuMFT.

Soubory vlastností a kódové stránky

Obsah všech souborů vlastností produktu Managed File Transfer musí zůstat v americké angličtině z důvodu omezení Java. Pokud upravíte soubory vlastností v jiném než americkém anglickém systému, musíte použít řídicí posloupnosti kódování Unicode.

z/OS Volby konfigurace produktu MFT v systému z/OS

Volby konfigurace produktu Managed File Transfer v systému z/OS jsou stejné jako volby pro distribuované platformy.

Další informace o volbách konfigurace v systému Multiplatformsviz “Volby konfigurace produktu MFT na platformách Multiplatforms” na stránce 648.

V systému z/OSje umístění konfigurace definováno proměnnou prostředí BFG_DATA. Pokud v adresáři UNIX System Services, na který odkazuje BFG_DATA, neexistuje žádná konfigurace, bude skript BFGCUSTM JCL s datovou sadou knihovny PDSE produktu MFT generovat úlohy nezbytné pro vytvoření konfigurace. Konfigurace se pak vytvoří, když spustíte tyto generované úlohy. Vytvoření konfigurace závisí na souboru BFG_DATA, který odkazuje na existující adresář, který je přístupný.

Můžete také vytvořit a spravovat konfiguraci pomocí stejných příkazů produktu **fte** , které jsou k dispozici v obou platformách Multiplatforms a z/OS. Seznam příkazů **fte** naleznete v části PříkazyMFT .

Windows V 9.1.0 Linux Konfigurace Redistributable Managed File Transfer Agent

Produkt Redistributable Managed File Transfer Agent můžete nakonfigurovat tak, aby se připojoval k existující infrastruktuře produktu IBM MQ a aby uživatelé mohli přenášet soubory, aniž byste museli instalovat produkt IBM MQ , abyste získali funkce produktu Managed File Transfer .

Než začnete

Informace o redistribuovatelných licenčních podmínkách pro produkt Redistributable Managed File Transfer Agentnajdete v části IBM MQ Redistribuovatelné komponenty.

Produkt Redistributable Managed File Transfer Agent poskytuje funkce produktu Managed File Transfer s těmito výjimkami:

- Připojení režimu vazeb ke koordinaci, příkazu a správcům front agentů není podporováno, je třeba použít připojení v režimu klienta. Když vydáváte příkazy, musíte poskytnout parametry, které jsou volitelné, když používáte produkt Managed File Transfer , který je nainstalován jako součást produktu IBM MQ: hostitel správce front, port, název a název kanálu.
- K dispozici nejsou následující příkazy:
  - fteCreateCDAgent.cmd
  - fteCreateLogger.cmd
  - fteDeleteLogger.cmd
  - fteMigrateLogger.cmd
  - fteSetLoggerTraceLevel.cmd
  - fteShowLoggerDetails.cmd
  - fteStartLogger.cmd
  - fteStopLogger.cmd

  Úplný seznam dostupných příkazů najdete v tématu Instalované sady příkazů MFT.
- Produkt Managed File TransferConnect:Direct není podporován.
- IBM MQ Explorer není zahrnuto.

Windows Chcete-li používat produkt Redistributable Managed File Transfer Agent, musíte na svém systému nainstalovat následující knihovny produktu Microsoft :

- Microsoft Visual C++ Redistributable 2008
- Microsoft Visual C++ Redistributable 2012

Tyto knihovny jsou k dispozici v produktu Microsoft. Viz Poslední podporované soubory ke stažení Visual C++.

Poznámka: Advanced Message Security není podporován v kombinaci s Redistributable Managed File Transfer package.

Informace o této úloze

Volitelně můžete produkt Redistributable Managed File Transfer Agent stáhnout a nakonfigurovat tak, aby se připojoval k existující infrastruktuře produktu IBM MQ , aby mohli uživatelé přenášet soubory mezi jejich lokálním prostředím a existující infrastrukturou produktu IBM MQ bez nutnosti instalace produktu IBM MQ. Chcete-li stáhnout a extrahovat Redistributable Managed File Transfer Agent, postupujte takto:

Postup

1. Stáhněte soubor IBM MQ znovu distribuovatelný balík agentů Managed File Transfer z produktu Fix Central.
   a) Vyberte balík pro váš operační systém:
   Názvy souborů archivu nebo ZIP popisují obsah souboru a ekvivalentní úrovně údržby.

   V 9.1.0 Například pro IBM MQ 9.1.0jsou názvy souborů následující:

   - Windows `9.1.0.0-IBM-MQFA-Redist-Win64`
   - Linux `9.1.0.0-IBM-MQFA-Redist-LinuxX64`

- Linux `9.1.0.0-IBM-MQFA-Redist-LinuxS390X`
- Linux `9.1.0.0-IBM-MQFA-Redist-LinuxPPC64LE`

b) Identifikujte adresář, do kterého chcete extrahovat balík, například:

- Windows `C:\MFTZ`
- Linux `/home/MFTZ`

2. Extrahujte obsah staženého balíku:

- Windows V systému Windowspoužijte nástroje produktu Windows Explorer k extrahování.
- Linux V systému Linux, extract a untar takto:

```
gunzip 9.0.1.0-IBM-MQFA-Redist-LinuxX64.tar.gz
```

a pak

```
tar xvf 9.0.1.0-IBM-MQFA-Redist-LinuxX64.tar
```

Vytvoří se následující adresáře:

- Windows Linux `bin`: Obsahuje všechny vyžadované příkazy produktu MFT .
- Windows `bin64`: Obsahuje požadované knihovny, které jsou potřebné pro podporu 64bitového operačního systému Windows
- Windows Linux `java`: Obsahuje knihovny IBM JRE a IBM MQ .
- Windows Linux `licenses`: Obsahuje soubory s licencemi
- Windows Linux `mqft`: Obsahuje adresáře `ant` a `lib` , které jsou vyžadovány pro podporu produktu Ant a pro podporu jádra produktu MFT
- Windows Linux `swtag`: Obsahuje soubor `swidtag` požadovaný správci licencí k identifikaci instalací v počítači.

Jak pokračovat dále

Nyní jste připraveni nakonfigurovat agenta MFT . Další kroky viz “Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Agent” na stránce 651.

Související pojmy

Možné chyby při konfiguraci agenta Redistributable MFT

Windows V 9.1.0 Linux Vytvoření počáteční konfigurace pro Redistributable Managed File Transfer Agent

Produkt Managed File Transfer Agent můžete nakonfigurovat tak, aby se připojoval k existující konfiguraci produktu IBM MQ .

Než začnete

Ujistěte se, že stáhnete a extrahujete obsah balíku produktu Redistributable Managed File Transfer Agent . Další informace viz téma “Konfigurace Redistributable Managed File Transfer Agent” na stránce 649.

Informace o této úloze

Nejprve vytvoříte prostředí, které potřebuje produkt Redistributable Managed File Transfer Agent . Pak můžete nastavit připojitelnost ke správci front, který běží na serveru IBM MQ , pak konfigurovat agenta a správce front agenta, před spuštěním a ověřením agenta.

Postup

1. Vytvořte prostředí pro produkt 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 staženého redistribuovatelného komponenty produktu MFT Agent. Spusťte tento příklad:

   - Windows

     ```
     fteCreateEnvironment.cmd -d datapath location
     ```

   - Linux

     ```
     . ./fteCreateEnvironment -d datapath location
     ```

   Tento příkaz přijímá následující nepovinné parametry:

   -d
   Tento parametr určuje umístění pro cestu k datům, kde je vytvořena, uložena a udržována konfigurace produktu MFT . Pokud spustíte příkaz **fteCreateEnvironment** bez určení umístění dat, vytvoří se adresář `mftdata` v umístění, kde je extrahováno 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.

   V 9.1.2 **-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:

   – Chcete-li rychle testovat novou funkci nebo funkci s použitím redistribuovatelného balíku s existující konfigurací, kde jsou agenti nakonfigurováni pro připojení ke správci front pouze v režimu klientů. (Všimněte si, že tento parametr se nevztahuje na žádného agenta, který je konfigurován pro připojení ke správci front v režimu vazeb.)

   – Provádíte-li migraci ze standardní instalace produktu Managed File Transfer do balíku produktu 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** naleznete v tématu fteCreateEnvironment (set up environment for Redistributable Managed File Transfer Agent).

   Proměnnou prostředí *BFG_DATA* můžete nastavit také s umístěním cesty k datům:

   ```
   BFG_DATA=Datapath location
   ```

   Před vytvořením, spuštěním a zastavením agenta nebo jinými příkazy se musíte ujistit, že proměnná *BFG_DATA* je nastavena na správné umístění cesty k datům.
2. Nastavení konektivity produktu IBM MQ .

a) Nastavte koordinačního správce front pomocí příkazu **fteSetupCoordination** .

Příkaz **fteSetupCoordination** vytvoří sadu, která je potřebná pro koordinaci správců front a adresářů potřebných pro další konfiguraci. Produkt Redistributable Managed File Transfer Agent pracuje v režimu klienta, takže s tímto příkazem musíte poskytnout další parametry, abyste se vyvarovali 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** naleznete v oddílu fteSetupCoordination. Informace o postupu konfigurace koordinačního správce front viz “Konfigurace koordinačního správce front pro produkt MFT” na stránce 688.

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** najdete v oddílu fteSetupCommands: create MFT command.properties file.

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.

V krocích “2” na stránce 652 a “3” na stránce 653 pro každého agenta vytvoříte definice front a témat ve správci front agenta.

4. Spusťte agenta a jste připraveni k přenosu souborů.

```
fteStartAgent -p PRMFTDEMO2 AGENT.TRI.BANK
```

Stav agenta můžete ověřit spuštěním následujícího příkazu:

```
fteListAgents
```

Další informace o použití příkazu **fteListAgents** naleznete v části fteListAgenti.

Související pojmy

“Konfigurace produktu Managed File Transfer” na stránce 647
Po instalaci můžete nakonfigurovat funkce produktu Managed File Transfer .

“Volby konfigurace produktu MFT na platformách Multiplatforms” na stránce 648
Produkt Managed File Transfer poskytuje sadu souborů vlastností, které obsahují klíčové informace o vašem nastavení a které jsou vyžadovány pro provoz. Tyto soubory vlastností se nacházejí v konfiguračním adresáři, který jste definovali při instalaci produktu.

Související odkazy

fteCreateTransfer: spuštění nového přenosu souboru

z/OS Vytvoření datové sady příkazu agenta nebo produktu Logger produktu MFT

You can create a PDSE data set of commands from the Managed File Transfer command template data set for a specific Managed File Transfer Agent or Managed File Transfer Logger for a specific coordination.

Informace o této úloze

Postupujte takto:

Postup

1. Vytvořte kopii datové sady knihovny DSFGCMDS se šablonou příkazu MFT PDSE s názvem souboru.

   z/OS SBFGCMDS musí být zkopírován do nové knihovny, například *prefix.agent*.JCL_. Můžete použít aktualizovanou verzi členu SBFGCMCMDS (BFGCOPY) s následujícími náhradníky:

   - Nahraďte *+ + supplied-library + +* úplným názvem SBFGCMCMDS PDSE.
   - z/OS Proměnný *+ + service-library + +* nahraďte úplným názvem nové datové sady knihovny PDSE příkazu MFT . *+ + service-library + +* je výstupní datová sada pro službu agenta nebo modulu protokolování, která je vytvořena.

2. Pro novou datovou sadu knihovny PDSE příkazu MFT upravte člen BFGCUSTM, což je skript JCL, abyste upravili příkazy pro agenta nebo modul protokolování. Každá proměnná je zadána ve formátu: *+ + název proměnné + +*, který musíte nahradit její požadovanou hodnotou. Popis různých proměnných JCL viz “Proměnné JCL z/OS” na stránce 666. 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 produktu MFT . Vlastnosti agenta a modulu protokolování můžete přidat podle potřeby, chcete-li upravit agenta nebo modul protokolování pro své prostředí. Seznam všech vlastností najdete v tématu “Soubory vlastností konfigurace” na stránce 677. Tato funkce je poskytována pro ukládání, které má přístup k souborům vlastností konfigurace produktu MFT , které jsou spravovány jako soubory systémových služeb UNIX .

   Prostředí definuje všechny dodatečně požadované vlastní proměnné prostředí.

3. Zadejte příkaz BFGCUSTM úlohy pro novou datovou sadu knihovny PDSE příkazu MFT . Tato úloha generuje sadu příkazů JCL, jako nové členy PDSE, vhodné pro agenta nebo registrátor. Úplný seznam příkazů viz “z/OS skripty JCL příkazů agenta a modulu protokolování” na stránce 670.

   Úloha BFGCUSTM aktualizuje knihovnu obsahující soubor JCL, který obsahuje příkaz DD s DISP=OLD. Po odeslání je třeba ukončit editor, aby bylo možné provést úlohu.

   Prozkoumejte protokol výstupní úlohy a zkontrolujte, zda byl skript JCL úspěšně spuštěn. Pokud dojde k selháním, opravte je a znovu odešlete úlohu BFGCUSTM.

   Skript BFGCUSTM JCL také aktualizuje soubory vlastností konfigurace produktu UNIX System Services MFT podle potřeby, aby bylo možné soubory uchovávat v kroku. Pokud konfigurace definovaná vlastností CoordinationQMgr neexistuje, jsou výstupem varovné zprávy a vy musíte spustit vygenerované úlohy BFGCFCR a BFGCMCR a vytvořit tak soubory vlastností konfigurace. Pro agenta musíte spustit BFGAGCR pro agenta a BFGLGCRS pro úpravu modulu protokolování. Pokud zadaná konfigurace již existuje, konfigurace se aktualizuje pomocí vlastností definovaných ve skriptu JCL BFTCUSTM.

Související pojmy

“Volby konfigurace produktu MFT v systému z/OS” na stránce 649
Volby konfigurace produktu Managed File Transfer v systému z/OS jsou stejné jako volby pro distribuované platformy.

Související úlohy

“Aktualizace existujícího datového souboru produktu MFT Agent nebo zapisovače protokolu na serveru z/OS” na stránce 665
Můžete aktualizovat datovou sadu knihovny PDSE příkazu Managed File Transfer , která je vytvořena z datové sady šablon příkazu Managed File Transfer .

z/OS Konfigurace produktu Managed File Transfer for z/OS

Produkt Managed File Transfer for z/OS vyžaduje přizpůsobení, aby mohla komponenta pracovat správně.

Informace o této úloze

Je třeba provést následující akce:

1. Úprava členu PDSE pro uvedení konfiguračních dat
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

“Kontrola konfigurace produktu MFT” na stránce 655
Než začnete, je třeba zkontrolovat konfiguraci systému.

Související úlohy

Instalace produktu Managed File Transfer for z/OS

z/OS Kontrola konfigurace produktu MFT

Než začnete, je třeba zkontrolovat konfiguraci systému.

Managed File Transfer (MFT) vyžaduje, aby jeden nebo více správců front jednal v následujících rolích pro každou definovanou konfiguraci MFT:

- Koordinační správce front, který uchovává informace o stavu jednotlivých agentů v konfiguraci publikované v rámci tématu koordinátora.
- Jeden nebo více správců front nebo správců front, kteří vystupují jako vstupní bod do sítě IBM MQ pro příkazy MFT.
- Jeden nebo více správců front agentů, kteří poskytují komunikaci mezi agentem MFT a sítí IBM MQ .

Každá z výše uvedených rolí může být prováděna samostatným správcem front nebo můžete tyto role kombinovat tak, aby v nejjednodušší konfiguraci byly všechny role prováděny jedním správcem front.

Pokud přidáváte správce front produktu z/OS do existujícího prostředí MFT, je nutné definovat konektivitu mezi správcem front produktu z/OS a ostatními správci front v konfiguraci. Toho lze dosáhnout s ručně definovanými přenosovými frontami nebo s použitím klastrování.

Každý agent MFT komunikuje s jedním správcem front. Pokud více agentů komunikuje se stejným správcem front, 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, ve kterých používáte profil, jako je `SYSTEM.FTE.COMMAND.*`, nebo můžete pro každého agenta definovat specifické profily.

Související pojmy

"Než začnete" na stránce 656

Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách produktu UNIX System Services (USS) a PDSE.

z/OS Než začnete

Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách produktu UNIX System Services (USS) a PDSE.

Většina z konfigurace a operace je prováděna pomocí jazyka JCL z PDSE a je třeba, abyste byli obeznámeni s prací v prostředí USS.

K OMVS můžete přistoupit z ISPF nebo můžete použít relaci typu Telnet pomocí příkazů na vaší pracovní stanici, například pomocí protokolu Telnet Putty nebo SSH.

Používáte-li OMVS z ISPF, můžete použít standardní editor ISPF a procházet příkazy **`oedit`** a **`obrowse`**.

Je třeba, abyste byli obeznámeni s následujícími příkazy USS

Tabulka 41. Běžné příkazy služeb systému UNIX

Příkaz	**Funkce**
chmod xxx cesta	Změňte přístupová oprávnění k souborům.
df -k cesta	Uvádí, kolik volného místa zůstává v systému souborů. Produkt -k hlásí volný prostor v kB.
cesta du -kt	Ohlašuje velikost adresářů pod cestou. Velikost hlášená v kB.
najít cestu -name xxx	Hledejte soubor s názvem `xxxx` v adresáři cesty. xxx je citlivý na velikost písmen a může být jako `*zzz`.
ls -ltrd adresář	Zobrazí informace o zadaném adresáři namísto souborů v adresáři.
ls -ltr cesta	Zobrazí informace o souborech v cestě.
obrowse název_souboru	Procházejte s názvem souboru.
Název souboru oedit	Upravte soubor v OMVS.

Zkontrolujte položky v následující tabulce a dokončete tabulku s příslušnými položkami pro váš podnik. Tyto hodnoty budete potřebovat při úpravě členu BFGCUSTM.

Tabulka 42. Parametry potřebné pro člen BFGCUSTM		
Název	**Příklad dat**	**Komentáře**
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 jako prázdný; například armELEMENT=	
armELEMTYPE	Pokud se používá ARM, použijte parametr ARM ELEMTYPE uvedený v zásadě ARM. Například armELEMTYPE= SYSBFGAG pro agenta nebo armELEMTYPE= SYSBFGLG pro registrátor. Pokud není služba ARM použita, nastavte tento parametr na prázdnou hodnotu; například armELEMTYPE=	
BFG_DATA		Dokončit podle potřeby
NÁZEV_SKUPINY_BFS	MQM	
DOMOVSKÁ STRÁNKA BFG_JAVA_HOME	`/java/java71_bit64_GA/J7.1_64/`	
VLASTNOSTI BFG_JVM_PROPERTIES		Dokončit podle potřeby
BF_PROD	`/var/ibm/wmqmft`	
BFG_WTO	YES	Chcete-li získat zprávu MFT na protokolu systému.
CLEAN_AGENT_PROPS	-trs	Tento parametr uvádí volby, které se použijí k vyčištění agenta při spuštění členu BFGAGCL. Další informace o platných hodnotách pro tento parametr naleznete v části fteCleanAgent: vyčištění agenta MFT.
coordinationQMgr	MQPV	Povinná konfigurace
CREDENTIAL_PATH		Používá se při migraci
Db2_HLQ	SYS2.Db2.V10	
CESTA_CESTY_DB		Používá se při migraci
FTE_CONFIG		Používá se při migraci
JOBCARD1		Jedná se o zakázkový list pro dlouho běžící úlohy, agenty a zapisovače protokolu.

Tabulka 42. Parametry potřebné pro člen BFGCUSTM (pokračování)		
Název	**Příklad dat**	**Komentáře**
KNIHOVNA	SCEN.FTE.JCL	Název datové sady MFT PDSE. Pro každou úlohu agenta nebo modulu protokolování je třeba zkopírovat kopii.
MQ_HLQ	Kvalifikátor vyšší úrovně pro datové sady produktu IBM MQ . Například: `MQM.V915`	
MQ_LANG	E	
CESTA_KE_MIME	`/mqm/V9R1M5`	
NAME	AGENT1	
VÝSTUPNÍ TŘÍDA	*	
Cesta	`bin:/usr/bin:/usr/sbin`	
productId	MFT	Tento parametr se používá k nastavení typu produktu, pro který se má zaznamenat použití produktu Managed File Transfer . Chcete-li získat informace o platných hodnotách pro tento parametr, prohlédněte si fteSetProductId: set z/OS SCRT recording product id.
QMGR	MQPV	
TYP_SLUŽBY	AGENT nebo LOGGER	
TMPDIR	`/tmp`	Přístup pro čtení a zápis v cestě USS pro dočasné soubory.

Kromě toho je třeba v případě potřeby zkontrolovat následující proměnné a dodat hodnoty:

- coordinationQMgrHostitel =
- coordinationQMgrPort =
- coordinationQMgrkanál =
- connectionQMgr=
- connectionQMgrHostitel =
- connectionQMgrPort =
- connectionQMgrKanál =

Tyto vlastnosti jsou společné pro AGENT nebo LOGGER.

Poznámka: Pro připojení klienta je nezbytný hostitel, port a kanál, ale pro připojení vazeb na lokálním počítači by mělo být ponecháno prázdné.

Související pojmy

“Položky ke kontrole” na stránce 659
Ujistěte se, že máte dostatek místa na disku, adresář pro ukládání dat a že požadované soubory existují.

“Úprava členu BFGCUSTM” na stránce 661
Musíte upravit člen BFGCUSTM a zadat hodnoty pro parametry, které váš podnik používá, než spustíte úlohu.

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 k dispozici dostatek místa na disku v systému souborů, do kterého chcete uložit specifické soubory konfigurace.

Je-li trasování agenta povoleno, pak standardně může použít 100 MB místa na disku.

Samotné konfigurační soubory jsou malé, pouze několik KB.

Pokud plánujete použít dva agenty a registrátor, potřebujete alespoň 300 MB. Můžete použít příkaz **df -k** `path`, kde `path` je umístění souborů specifických pro instalaci. To dává dostupným a celkový prostor v kB.

300 MB je 307,200 KB, takže byste měli povolit alespoň 310.000 KB

Vytvořit a zkontrolovat adresář pro ukládání dat produktu Managed File Transfer

Potřebujete adresář pro uložení dat produktu Managed File Transfer (MFT).

Zkontrolujte, zda je v systému souborů dostatek místa `df -k /var`. Tento systém souborů by měl mít k dispozici alespoň 310.000 kB.

Pokud jste tento systém souborů nevytvořili, použijte příkaz **mkdir** ; například **mkdir /var/mft**.

Zobrazte, jaká oprávnění mají uživatelé v tomto adresáři, pomocí příkazu **ls -ltrd /var/mft**.

Není-li vlastník nebo skupina správná, použijte příkaz **chown owner:group /var/mft**.

Nejsou-li oprávnění ke skupině správná, udělte vlastníkovi a skupině oprávnění ke čtení, zápisu a provádění skupině oprávnění ke čtení, zápisu a provádění. Všimněte si, že následující příkaz také dává všem uživatelům oprávnění ke čtení a provádění **chmod 775 /var/mft**.

Zkontrolujte, zda soubory existují a máte k nim 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 přístup pro čtení, zápis a provádění do tohoto adresáře.

p-x
Osoby ve skupině *TSOUSER* mohou číst a provádět soubory v adresáři.

p-x
Univerzální přístup, to znamená, že kdokoli může číst nebo provádět soubory v adresáři.

Zkontrolujte soubory uvedené v:

Tabulka 43. Přístup požadovaný uživateli k určitým souborům	
Cesta	**Přístup požadovaný uživateli, kteří provádějí konfiguraci**
DOMOVSKÁ STRÁNKA BFG_JAVA_HOME	Čtení a provádění
/tmp	Čtení a zápis
BF_PROD	Číst
BFG_DATA	Zapisovat
CESTA_KE_MIME	Číst

Související pojmy

“Než začnete” na stránce 656
Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách produktu UNIX System Services (USS) a PDSE.

“Obecné konfigurace produktu MFT for z/OS” na stránce 660
Přehled různých konfigurací produktu Managed File Transfer

z/OS Obecné konfigurace produktu MFT for z/OS

Přehled různých konfigurací produktu Managed File Transfer

Produkt Managed File Transfer používá agenty připojené ke správci front za účelem přenosu dat.

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 konfigurující MFT musí rozumět službám USS (Unix System Services). Příklad:
   - Adresářová struktura se soubory, které mají názvy jako `/u/userID/myfile.txt2`
   - Příkazy USS jako 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 USS nezbytné, aby bylo možné nakonfigurovat a provozovat MFT:
   - Java; například `/java/java71_bit64_GA/J7.1_64/`
   - IBM MQ V800, například `/mqm/V8R0M03`.

- Knihovny JDBC Db2, pokud chcete použít Db2 pro stav a historii, například `/db2/db2v10/jdbc/lib`

Potřebujete koordinačního správce front. Stejného správce front však můžete používat ke spouštění agentů, ke zpracování příkazů a ke koordinaci. Pokud používáte více správců front, je třeba vybrat jeden z nich, který bude koordinátorem.

Zkontrolujte konektivitu produktu IBM MQ

Máte-li existujícího správce front koordinátora produktu MFT , je třeba provést konektivitu mezi správcem front, ve kterém provádíte konfiguraci, a koordinací a správci front příkazů.

z/OS Kopírovat SBFGCMDS pro vytvoření knihovny JCL

Pro každého agenta a modul protokolování je třeba vytvořit knihovnu JCL. JCL obsahuje konfiguraci a úlohy použité k vytvoření a spuštění agenta nebo zapisovače protokolu.

Pro každého agenta a modul protokolování vytvořte kopii knihovny SBFGCMCMDS dodávaného produktem IBM úpravou a spuštěním členu BFGCOPY.

Tato knihovna se používá k definování konfigurace pro agenta nebo pro modul protokolování a po přizpůsobení obsahuje úlohy, které lze použít k vytvoření požadované konfigurace a agenta nebo modulu protokolování produktu Managed File Transfer .

Člen BFGCUSTM v rámci tohoto procesu vytvoříte jako člen.

Poznámka: Pokud jste obeznámeni s příkazy USS, můžete produkt z/OS nakonfigurovat se stejnými příkazy, které používáte na jiných platformách.

Související pojmy

“Obecné konfigurace produktu MFT for z/OS” na stránce 660
Přehled různých konfigurací produktu Managed File Transfer

“Úprava členu BFGCUSTM” na stránce 661
Musíte upravit člen BFGCUSTM a zadat hodnoty pro parametry, které váš podnik používá, než spustíte úlohu.

z/OS Úprava členu BFGCUSTM

Musíte upravit člen BFGCUSTM a zadat hodnoty pro parametry, které váš podnik používá, než spustíte úlohu.

Seznam parametrů vyžadujících specifické hodnoty naleznete v části Parametry potřebné pro člen BFGCUSTM.

Kromě toho je třeba v případě potřeby zkontrolovat následující proměnné a dodat hodnoty:

- coordinationQMgrHostitel =
- coordinationQMgrPort =
- coordinationQMgrkanál =
- connectionQMgr=
- connectionQMgrHostitel =
- connectionQMgrPort =
- connectionQMgrKanál =

Tyto vlastnosti jsou společné pro AGENT nebo LOGGER.

Poznámka: Pro připojení klienta je nezbytný hostitel, port a kanál, ale pro připojení vazeb na lokálním počítači by mělo být ponecháno prázdné.

Pokud se jedná o prvního správce front ve vašem prostředí Managed File Transfer a chcete pro koordinaci, příkazy a spuštěné agenty použít stejného správce front, nastavte hodnoty na název lokálního správce front.

```
coordinationQMgr=MQPV
connectionQMgr=MQPV
```

kde MQPV je název vašeho lokálního správce front.

Odešlete úlohu, která aktualizuje PDSE, a vytvoří adresářovou strukturu pod zadanou cestou.

Všimněte si, že tato úloha vyžaduje výlučné použití, takže musíte přestat používat PSDE, zatímco je úloha spuštěna.

Rada: Kdykoli odešlete úlohu BFGCUSTM, úloha nahradí všechny soubory JCL. Každý člen, kterého změníte, byste měli přejmenovat.

Související pojmy

“Než začnete” na stránce 656
Konfigurace produktu Managed File Transfer (MFT) používá soubory v datových sadách produktu UNIX System Services (USS) a PDSE.

“Vytvoření agenta” na stránce 664
Musíte zkopírovat PDSE, chcete-li provést PDSE specifickou pro agenta, například *user.MFT.AGENT1*. Zkopírujte PDSE z předchozí konfigurace agenta nebo modulu protokolování, pokud existují. Je-li to vaše první konfigurace, zkopírujte PDSE dodané s MFT.

z/OS Definování koordinačního správce front

Produkt Managed File Transfer vyžaduje vytvoření správce front, který slouží jako koordinační správce front.

V závislosti na konfiguraci, kterou jste vybrali, je tento správce front na lokálním systému MVS nebo na jiném počítači. V prvním případě jsou připojení k serveru vazeb a v druhém případě jsou to připojení klienta.

Po úspěšném spuštění kroku konfigurace jsou v PDSE úspěšně nakonfigurovány členy.

Člen BFGCFCR definuje koordinačního správce front a tuto úlohu:

1. Vytvoří adresářovou strukturu v adresáři Managed File Transfer (MFT) a vytvoří konfigurační soubory.
2. Spustí CSQUTIL pro definování prostředků IBM MQ .

Je-li koordinační správce front na vzdáleném počítači, pak tento krok úlohy selže.

Člen BCFCFCR vytváří soubory v USS a vytváří definice MQ . Tato úloha:

1. Vytvoří téma MFT,
2. Vytvoří frontu MFT
3. Alters *NAMELIST (SYSTEM.QPUBSUB.QUEUE.NAMELIST)* jako názvy *NAMES (SYSTEM.BROKER.DEFAULT.STREAM, SYSTEM.BROKER.ADMIN.STREAM, SYSTEM.FTE)*
4. Provádí příkaz *ALTER QMGR PSMODE (ENABLED)* .

   Zobrazí se *DISPLAY NAMELIST (SYSTEM.QPUBSUB.QUEUE.NAMELIST)* příkaz byl vydán před provedením změny. Pokud váš formát NAMLIST není výchozí, měli byste změnit svůj seznam jmen a přidat SYSTEM.FTE do vašeho seznamu názvů

Přejmenujte člen BCFCFCR s vlastní předponou, například CCPCFCR, protože znovu přizpůsobujete tento soubor.

Upravte tento přejmenovaný člen vložením názvu vašeho souboru pověření. Příklad:

```
%BFGCMD CMD=fteSetupCoordination +
-credentialsFile //'<MFTCredentialsDataSet(MemberName)>'
```

Uložte a odešlete úlohu. Uvědomte si, že pokud potřebujete znovu odeslat úlohu, je třeba přidat volbu *-f* .

Když se tato úloha spustí, vypíše IBM MQ prostředky, které vytvoří. Tyto prostředky je třeba 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 663
Jako správce front pro koordinaci a správce front můžete buď použít stejného správce front, nebo můžete vytvořit nového správce front příkazů.

z/OS Definování správce front příkazů

Jako správce front pro koordinaci a správce front můžete buď použít stejného správce front, nebo můžete vytvořit nového správce front příkazů.

Informace o této úloze

Musíte mít správce front příkazů, nicméně pro koordinaci a správce front příkazů můžete použít stejného správce front. V opačném případě je třeba vytvořit nového správce front příkazů. To může být na stejném počítači jako koordinační správce front, ale nemusí být.

Postup

1. Přejmenujte člen BFGCMCR s vlastní předponou, např. CCPCMCR.

   Musíte přejmenovat BFGCMCR, protože znovu upraví tento soubor.
2. Upravte přejmenovaný člen tak, že vložíte název souboru pověření.

   Příklad:

   ```
   %BFGCMD CMD=fteSetupCommands +
   -credentialsFile //'<MFTCredentialsDataSet(MemberName)>' +
   ```
3. Uložte a odešlete úlohu.

   Uvědomte si, že pokud potřebujete znovu odeslat úlohu, je třeba přidat volbu *-f* .

   Tento správce front se používá pro příkazy jako např. **ftePingAgent**.
4. Zkontrolujte tento člen, odešlete jej, a přezkoumejte výstup.

Jak pokračovat dále

Informace o tom, jak vytvořit agenta, viz “Vytvoření agenta” na stránce 664 .

Související pojmy

“Definování koordinačního správce front” na stránce 662
Produkt Managed File Transfer vyžaduje vytvoření správce front, který slouží jako koordinační správce front.

Související úlohy

Konfigurace MQMFTCredentials.xml

Související odkazy

Formát souboru pověření MFT

z/OS Vytvoření agenta

Musíte zkopírovat PDSE, chcete-li provést PDSE specifickou pro agenta, například *user.MFT.AGENT1*. Zkopírujte PDSE z předchozí konfigurace agenta nebo modulu protokolování, pokud existují. Je-li to vaše první konfigurace, zkopírujte PDSE dodané s MFT.

Zkontrolujte člen BFGCUSTM a v případě, že potřebujete použít jiný soubor pověření, vytvořte jej.

Většina obsahu zůstává stejná z přizpůsobení, která je podrobně popsána v části “Úprava členu BFGCUSTM” na stránce 661.

Musíte změnit:

- // SYSEXEC DD DSN=SCEN.FTE.JCL.AGENT1
- KNIHOVNA odpovídá agentovi PDSE
- SERVICE_TYPU = AGENT
- Název jako název agenta (odpovídající hodnotě PDSE) JOBCARD
- Změňte BFG_JVM_PROPERTIES = "-Xmx1024M"

Odešlete tuto úlohu a pamatujte si, že úloha vyžaduje výlučný přístup k datové sadě.

Úlohy pro agenta mají všechny názvy ve formátu *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. Uveďte název vašeho souboru pověření, například `-credentialsFile //'SCEN.FTE.JCL.VB(CREDOLD)`. Pokud neuvedete název, úloha pro spuštění agenta nevyužívá soubor pověření.

Zkontrolujte výstup a ujistěte se, že byl proces úspěšně spuštěn.

Rada: Zkopírujte název cesty souboru *agent.properties* z výstupu úlohy do členu v PDSE pro agenta.

Například zkopírujte `/u/userid/fte/wmqmft/mqft/config/MQPA/agents/AGENT1/agent.properties` do členu AGENT.

To je užitečné v případě, že potřebujete zobrazit soubor vlastností a přidat řádek `/u/userid/fte/wmqmft/mqft/logs/MQPA/agents/AGENT1/logs`.

To je místo, kde jsou uloženy trasovací soubory.

Související pojmy

“Definování koordinačního správce front” na stránce 662
Produkt Managed File Transfer vyžaduje vytvoření správce front, který slouží jako koordinační správce front.

“Použití agenta” na stránce 664
Jak použijete různé příkazy k ujištění, že agent pracuje správně.

Související úlohy

“Definování správce front příkazů” na stránce 663
Jako správce front pro koordinaci a správce front můžete buď použít stejného správce front, nebo můžete vytvořit nového správce front příkazů.

z/OS Použití agenta

Jak použijete různé příkazy k ujištění, že agent pracuje správně.

Spuštění agenta

Přejmenujte člena BFGAGST, přezkoumejte člen a odešlete úlohu.

Pokud vám tato zpráva funguje, obdržíte zprávu BFGAG0059I: Agent byl úspěšně spuštěn.

Zobrazit aktivního agenta (y)

Přejmenujte člen BFGAGLI, zkontrolujte člen a odešlete úlohu, která používá koordinačního správce front.

Je třeba vyřešit všechny problémy s připojením.

PING na agenta pro kontrolu, zda funguje

Přejmenujte člena BFGAGPI, zkontrolujte člen a odešlete úlohu, která používá správce front příkazů.

Je třeba vyřešit všechny problémy s připojením.

Provést přenos testu

Další informace viz “Provedení přenosu verifikace” na stránce 672.

Zastavení agenta

Přejmenujte člen BFGAGSP, přezkoumejte člen a odešlete úlohu.

Restartujte agenta pomocí člena BFGAGST.

Související pojmy

“Vytvoření agenta” na stránce 664
Musíte zkopírovat PDSE, chcete-li provést PDSE specifickou pro agenta, například *user.MFT.AGENT1*. Zkopírujte PDSE z předchozí konfigurace agenta nebo modulu protokolování, pokud existují. Je-li to vaše první konfigurace, zkopírujte PDSE dodané s MFT.

z/OS Aktualizace existujícího datového souboru produktu MFT Agent nebo zapisovače protokolu na serveru z/OS

Můžete aktualizovat datovou sadu knihovny PDSE příkazu Managed File Transfer , která je vytvořena z datové sady šablon příkazu Managed File Transfer .

Postup

1. Upravte člen skriptu JCL BFGCUSTM a aktualizujte proměnné a vlastnosti v příkazu BFGSTDIN DD.

   Chcete-li odstranit vlastnost, která byla dříve definována, nastavte její hodnotu na prázdnou, místo odebrání položky. Když se spustí skript BFGCUSTM JCL, uvedené vlastnosti se použijí jako aktualizace skutečného agenta a protokolování souborů vlastností produktu UNIX System Services; nastavení vlastnosti na prázdnou hodnotu označuje, že vlastnost má být odebrána
2. Odešlete úlohu BFGCUSTM. Tato úloha znovu vygeneruje sadu příkazů JCL, která odpovídá agentovi nebo registrátoru. Úplný seznam příkazů viz “z/OS skripty JCL příkazů agenta a modulu protokolování” na stránce 670. Prozkoumejte protokol výstupní úlohy a zkontrolujte, zda byl skript JCL úspěšně spuštěn. Pokud dojde k selháním, opravte je a znovu odešlete úlohu BFGCUSTM.

Výsledky

Generované skripty JCL můžete upravit a přidat svou vlastní logiku. Když však znovu spustíte BFGCUSTM, buďte opatrní, protože můžete přepsat vlastní logiku.

Související pojmy

“Volby konfigurace produktu MFT v systému z/OS” na stránce 649
Volby konfigurace produktu Managed File Transfer v systému z/OS jsou stejné jako volby pro distribuované platformy.

Související úlohy

“Vytvoření datové sady příkazu agenta nebo produktu Logger produktu MFT” na stránce 653
You can create a PDSE data set of commands from the Managed File Transfer command template data set for a specific Managed File Transfer Agent or Managed File Transfer Logger for a specific coordination.

z/OS *Proměnné JCL z/OS*

Ve skriptu BFGCUSTM můžete použít substituční hodnoty, proměnné JCL a vlastnosti konfigurace.

V následující tabulce jsou uvedeny substituční hodnoty pro skript BFGCUSTM JCL v datové sadě knihovny PDSE příkazu MFT . Před odesláním úlohy BFGCUSTM je třeba nahradit tyto substituční hodnoty vhodnými hodnotami.

Tabulka 44. 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 .
+ + bfg_prod + +	Umístění instalačního adresáře produktu UNIX System Services v produktu MFT .

V následující tabulce jsou popsány 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 zadané substitučními hodnotami (to znamená hodnoty uzavřené ve dvou znamének plus, + +), s vhodnými hodnotami.

Tabulka 45. Proměnné prostředí

Proměnná prostředí	**Hodnota**
KNIHOVNA	Název datové sady obsahující knihovny PDSE příkazu MFT .
TMPDIR	UNIX Systémový adresář služeb pro dočasné soubory.
BF_PROD	Umístění instalačního adresáře produktu UNIX System Services v produktu MFT .
BFG_DATA	Umístění datového adresáře pro Managed File Transfer for z/OS, což je cesta k *DATA_DIR*.
DOMOVSKÁ STRÁNKA BFG_JAVA_HOME	Umístění instalace produktu Java .
VLASTNOSTI BFG_JVM_PROPERTIES	Volitelné. Nastaví hodnotu pro proměnnou prostředí BFG_JVM_PROPERTIES. Tyto vlastnosti jsou předány virtuálnímu počítači Java .

Tabulka 45. Proměnné prostředí (pokračování)

Proměnná prostředí	**Hodnota**
NÁZEV_SKUPINY_BFS	Skupina souborů mqm je obvykle asociována s konfiguračními datovými soubory a příkazy konfigurace produktu MFT . Consequently, all users who are members in the mqm group can access and make changes to the MFT configuration. Další informace naleznete v tématu Oprávnění systému souborů pro MFT v IBM MQ. Pro systém z/OS je skupina souborů entitou systému souborů USS a skupina souborů mqm není nutně definována. Skupinu systémů souborů z/OS USS pro konfigurační datové soubory produktu MFT můžete přidružit pomocí proměnné prostředí BFG_GROUP_NAME. Například při použití výzvy shellu USS: `export BFG_GROUP_NAME=FTEGB` který definuje skupinu *FTEGB* , která má být přidružena k jakýmkoli následně vytvořeným konfiguračním souborům pro aktuální relaci USS. Hodnotu BFG_GROUP_NAME můžete nastavit na prázdnou hodnotu, nebo ji můžete odebrat. **Poznámka:** Při prvním spuštění souboru BFGCUSTM, pokud má být konfigurace produktu MFT použita více ID uživatele, je důležité, aby proměnná BFG_GROUP_NAME byla nastavena na skupinu, která je přístupná pro všechny požadované ID uživatele. Je-li znovu spuštěn BFGCUSTM, nesmí být proměnná BFG_GROUP_NAME změněna (jinak se musí změnit oprávnění souboru skupiny USS pro všechny soubory a adresáře v adresáři, na který odkazuje BFG_DATA), aby bylo možné zohlednit nové nastavení BFG_GROUP_NAME). Spustíte-li příkaz **fteMigrateAgent** na systému z/OS s proměnnou prostředí BFG_GROUP_NAME nastavenou na neprázdnou hodnotu, příkaz zkontroluje, zda je uživatel členem skupiny pojmenované proměnnou BFG_GROUP_NAME. Není-li uživatel členem pojmenované skupiny, může příkaz nahlásit chybovou zprávu `BFGCL0502E: Nemáte oprávnění k provedení požadované operace.` a nespustí se. Podrobné informace o kritériích, které musí uživatel splnit, aby úspěšně spustil tento příkaz, naleznete v tématu fteMigrateAgent .

Tabulka 45. Proměnné prostředí (pokračování)	
Proměnná prostředí	**Hodnota**
BFG_WTO	Protokolování z/OS je povoleno, je-li hodnota BFG_WTO nastavena na hodnotu YES, ON nebo TRUE. To řídí, zda se zprávy, které jsou zapsány do protokolu událostí agenta, zapisují také do protokolovacího zařízení obsluhy z/OS , které umožňuje snadnější přístup k automatizovaným produktům, když spustíte agenta z JCL. Směrovací kód je Programmer Information (11) a kód deskriptoru je Informační (12).
TYP_SLUŽBY	Určuje, zda je knihovna příkazů MFT určena pro agenta nebo modul protokolování. Platné hodnoty jsou AGENT nebo LOGGER.
NAME	Název agenta nebo zapisovače protokolu pro hodnotu SERVICE_TYPE.
QMGR	Název lokálního správce front, který je přidružen k agentovi nebo registrátoru pro hodnotu SERVICE_TYPE.
VÝSTUPNÍ TŘÍDA	Třída výstupu pro datové sady SYSOUT. Předvolba je *, která požaduje stejnou výstupní třídu jako parametr MSGCLASS z příkazu úlohy.
CESTA_KE_MIME	Používá se v souboru BFGPROF k vytvoření proměnné prostředí LIBPATH.
MQ_HLQ	Kvalifikátor vyšší úrovně pro datové sady produktu IBM MQ .
MQ_LANG	Jazyk, který je povinný.
DB2_HLQ	Volitelné. Kvalifikátor nejvyšší úrovně pro datové sady produktu Db2 .
JOBCARD1	Řádek záhlaví 1 pro úlohu příkazu JCL.
JOBCARD2	Řádek záhlaví 2 pro úlohu příkazu JCL.
JOBCARD3	Řádek záhlaví 3 pro příkazovou úlohu JCL.
ADMIN_JOB1	Řádek záhlaví 1 pro úlohu administrátora.
ADMIN_JOB2	Řádek záhlaví 2 pro úlohu administrátora.
ADMIN_JOB3	Řádek záhlaví 3 pro úlohu administrátora.
FTE_CONFIG	Existující konfigurace produktu WMQFTE pro migraci. Pokud migrace není povinná, nastavte ji na prázdnou hodnotu.

Tabulka 45. Proměnné prostředí (pokračování)	
Proměnná prostředí	**Hodnota**
CREDENTIAL_PATH	Cesta k souboru pověření pro migraci, například `/u/user1/agent3`. Soubory pověření pro migraci pro produkt Managed File Transfer musí být umístěny v samostatném souboru ke konfiguraci informací o konfiguraci a konfiguračních souborech v produktu IBM WebSphere MQ File Transfer Edition 7.0.4.4. Nezbytné pouze pro příkazy migrace **BFGAGMG** a skripty JCL **BFGLGMG** . Pokud migrace není povinná, nastavte ji na prázdnou hodnotu.
CESTA_CESTY_DB	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`. Pokud migrace není povinná, nastavte ji na prázdnou hodnotu.

Poznámka: Soubory jar produktu IBM MQ se dodávají s MFT, v adresáři *`MQMFT product root`*`/java/lib`, jsou vždy používány a nejsou konfigurovatelné.

Následující tabulka popisuje povinné vlastnosti konfigurace produktu 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 (to znamená hodnoty uzavřené mezi dvěma znaky plus a + +) s vhodnou neprázdnou hodnotou. Tyto vlastnosti definují přepisy pro vlastnosti konfigurace produktu MFT . Můžete přidat vlastnosti agenta a zapisovače protokolu, chcete-li upravit agenty nebo zapisovače protokolu pro vaše prostředí. Seznam všech vlastností najdete v tématu “Soubory vlastností konfigurace” na stránce 677.

Tabulka 46. Povinné konfigurační vlastnosti pro příkaz BFGSTDIN DD	
Vlastnost	**Hodnota**
coordinationQMgr	Název koordinačního správce front pro konfiguraci, ke které je přidružen agent nebo modul protokolování.
Hostitel coordinationQMgr	Volitelné. Název hostitele systému, na kterém je spuštěn koordinační správce front. Ponecháte-li hodnotu této vlastnosti prázdnou, bude se předpokládat připojení v režimu vázání.
Port coordinationQMgr	Volitelné. Číslo portu, na kterém koordinující správce front naslouchá. Tento parametr se používá pouze v případě, že jste také zadali neprázdnou hodnotu pro vlastnost Hostitel coordinationQMgr.
Kanál coordinationQMgr	Volitelné. Kanál, který má být použit pro připojení ke koordinačnímu správci front. Tento parametr se používá pouze v případě, že jste také zadali neprázdnou hodnotu pro vlastnost Hostitel coordinationQMgr.
connectionQMgr	Název správce front příkazů pro konfiguraci, ke které je přidružen agent nebo modul protokolování.

Tabulka 46. Povinné konfigurační vlastnosti pro příkaz BFGSTDIN DD (pokračování)	
Vlastnost	**Hodnota**
connectionQMgrHostitel	Volitelné. Název hostitele systému, na kterém běží správce front příkazů. Ponecháte-li hodnotu této vlastnosti prázdnou, bude se předpokládat připojení v režimu vázání.
connectionQMgrPort	Volitelné. Číslo portu, na kterém naslouchá správce front příkazů. Tento parametr se používá pouze v případě, že jste pro vlastnost hostitele connectionQMgrzadali také neprázdnou hodnotu.
connectionQMgrkanál	Volitelné. Kanál, který má být použit pro připojení ke správci front příkazů. Tento parametr se používá pouze v případě, že jste pro vlastnost hostitele connectionQMgrzadali také neprázdnou hodnotu.

z/OS *z/OS skripty JCL příkazů agenta a modulu protokolování*

Sada příkazů JCL, která jsou k dispozici v datové sadě knihovny PDSE příkazu MFT .

Tabulka 47. Příkazy JCL dostupné v datové sadě knihovny PDSE příkazu MFT	
Člen	**Popis nebo příkaz fte na příkazovém řádku**
BFGCOPY	Úloha pro vytvoření kopie této knihovny
BFGCUSTM	Úloha pro úpravu této knihovny pro agenta nebo modul protokolování
BFGCFCR	fteSetupKoordinace
BFGCMCR	Příkazy pro fteSetup: vytvoření souboru MFT command.properties
BFGMAGR	fteCreateAgent. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGLGCRY	fteCreateLogger. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.
BFGAGSTCITY	fteStartAgent. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGAGSTP	**fteStartAgent** . Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGAGPI	ftePingAgent. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGAGSP	fteStopAgent. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGLGST	fteStartLogger. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.
BFGGSTP	**fteStartLogger** . Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.
BFGLGSP	fteStopLogger. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.

Tabulka 47. Příkazy JCL dostupné v datové sadě knihovny PDSE příkazu MFT (pokračování)	
Člen	**Popis nebo příkaz fte na příkazovém řádku**
BFGAGSHCH	fteShowAgentDetails. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGLGSHK	fteShowLoggerDetails. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.
BFGCFDF	fteChangeDefaultConfigurationVolby
BFGAGCL	AgentfteClean. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGAGDEOVÁ	fteDeleteAgent. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGLGDE	fteDeleteLogger. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.
BFGPRSH	fteDisplayVerze
BFGAGLI	fteListAgenti. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGMNLI	fteListMonitory
BFGSTLI	fteListScheduledTransfers
BFGTMLI	fteListšablon
BFGAGMG	**fteMigrateAgent**. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGLGMG	**fteMigrateLogger**. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.
BFGCROBS	**fteObfuscate** ukázka
BFGZRAS	**fteRAS**
BFGAGTC	fteSetAgentTraceÚroveň. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na AGENT.
BFGGTC	fteSetLoggerTraceÚroveň. Vytvoří se pouze tehdy, když nastavíte proměnnou SERVICE_TYPE na LOGGER.
BFGPRANS	**fteAnt** ukázka
BFGTRCAS	**fteCancelTransfer** ukázka
BFGMTCRS	**fteCreateMonitor** ukázka
BFGTMCRS	**fteCreateTemplate** ukázka
BFGTRCR	**fteCreateTransfer** ukázka
BFGMNDY	**fteDeleteMonitor** ukázka
BFGSTDES	**fteDeleteScheduledTransfer** ukázka
BFGTDES	**fteDeleteTemplates** ukázka

Notes:

- JCL, pro příkazy, které vytvářejí skripty MQSC nebo odkazují na odstranění skriptů, vás požádá o spuštění skriptu, ale tento skript již byla spuštěna úlohou.
- BFGZRAS vytvoří člen BFGRAS, když se spustí úloha BGCUSTM.

z/OS Provedení přenosu verifikace

Jak jste provedli přenos, abyste zkontrolli, že produkt pracuje správně.

Přejmenovat a upravit člen BFGTRS.

1. Přidejte `/*` před `%BFGCMD CMD=fteCreateTransfer -h`
2. Odeberte ostatní komentáře v členu.
3. Uveďte aktuální název agenta pro `-sa` a `-da`
4. Uložit JCL
5. Odeslat JCL

Tento skript JCL se připojuje ke správci front příkazů.

z/OS Konfigurace úlohy protokolování

Úloha protokolování musí být spuštěna na stejném obrazu jako koordinačního správce front. Můžete se přihlásit k produktu Db2.

Vytvoření úlohy protokolování

Zkopírujte PDSE, abyste učinili modul protokolování specifickou pro modul PDSE. Například `user.MFT.LOGGER`.

Potřebujete-li použít jiný soubor pověření, vytvořte jej. Další informace viz Konfigurace MQMFTCredentials.xml na systému z/OS.

Zkontrolujte člena BFGCUSTM. Všimněte si, že velká část obsahu zůstává stejná od předchozího přizpůsobení.

Je však třeba:

- Změňte // SYSEXEC DD DSN=SCEN.FTE.JCL....
- Změňte parametr LIBRARY tak, aby odpovídal agentovi PDSE
- Změňte správce front na název koordinačního správce front.
- Nastavit SERVICE_TYPE=LOGER
- Změňte název NAME, aby byl názvem modulu protokolování (odpovídá PDSE)
- Zkontrolujte úlohu JOBCARD a změňte název úlohy tak, aby se název lišil od názvů úloh agentů.
- Zkontrolujte BFG_JVM_PROPERTIES = "-Xmx1024M"

Pokud používáte modul protokolování produktu Db2 , je užitečný k vytvoření souboru, abyste mohli zachytit trasování produktu Db2 , které vám pomohou identifikovat problémy s produktem Db2 .

Název souboru je určen ve vlastnostech prostředí JVM, kde má soubor vlastností trasování JDBC obsah, jako je například

```
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 a všimněte si, že úloha vyžaduje výlučný přístup k datové sadě. Všechny úlohy pro agenta mají názvy jako *BFGLG**.

Protokolování do souborů

Další informace o přihlášení k produktu Db2naleznete v tématu “Vytvoření úlohy protokolování, když se přihlašuje k produktu Db2” na stránce 673 .

Přejmenovat člen 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 uvádí syntaxi příkazu.

To create the logger task comment out the `%BFGCMD CMD=fteCreateLogger -h` by putting `/*` in front of the statement, making sure that column one is blank.

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 se úspěšně zpracoval.

Tip: Zkopírujte název cesty souboru `logger.properties` z výstupu úlohy do členu v PDSE na agentovi.

Například kopírování do členu APATH

```
/u/user_ID/fte/wmqmft/mqft/config/MQPH/loggers/LOGGER/logger.properties
```

To je užitečné v případě, že potřebujete zobrazit soubor vlastností.

Přidejte adresář do tohoto souboru:

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/
```

Pokud se přihlašujete k souboru, jsou soubory protokolu uloženy v tomto adresáři, například `LOGGER0-20140522123654897.log`.

Trasovací soubory jsou umístěny v podadresáři protokolů, například

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/logs
```

Nyní můžete spustit úlohu protokolování.

Vytvoření úlohy protokolování, když se přihlašuje k produktu Db2

Přejmenovat člen BFGLGCRS.

Tato úloha aktualizuje soubory v adresáři MFT a používá CSQUTIL k vytvoření front specifických pro agenta v lokálním správci front.

Musíte vědět:

Tabulka 48. Db2 proměnné	
Název Db2	**Příklad**
-dbName databaseName	Tuto hodnotu můžete získat od hodnoty umístění ve zprávě DSNL004I pro váš 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 uvádí 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
```

To create the logger task comment out the `%BFGCMD CMD=fteCreateLogger -h` by putting `/*` in front of the statement, making sure that column one is blank.

Odešlete úlohu a zkontrolujte výstup, abyste viděli, že se úspěšně zpracoval.

Tip: Zkopírujte název cesty souboru `logger.properties` z výstupu úlohy do členu v PDSE z agentů.

Například kopírování 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 umístěny v podadresáři protokolů, například:

```
/u/user_ID/fte/wmqmft/mqft/logs/MQPH/loggers/LOGGER/logs
```

Vytváření tabulek Db2

Je třeba vytvořit tabulky Db2 . Definice jsou v souboru USS `mqft/sql/ftelog_tables_zos.sql`.

Vytvořte člen Db2 ve vaší PDSE. Upravte tento člen a použijte příkaz COPY na příkazovém řádku. Kopírovat ze souboru definic USS.

Protože požadavky specifické pro server se mohou výrazně lišit, tento soubor určuje pouze základní struktury tabulek a tabulkový prostor, ve kterém budou umístěny.

Tabulkový prostor je určen skriptem SQL, aby se zajistilo, že je vytvořen pomocí fondu vyrovnávacích pamětí s velikostí stránky, která je dostatečná pro uchování největších řádků tabulek. Všimněte si, že atributy jako např. umístění objektů LOB a tak dále nejsou zadány.

Administrátor vaší databáze může chtít upravit kopii tohoto souboru, abyste mohli definovat tyto atributy související s výkonem.

Tento soubor také předpokládá výchozí název schématu produktu FTEL0G, výchozí název tabulkového prostoru FTEL0GTSa název databáze FTEL0GDB. Tyto názvy můžete změnit, pokud potřebujete, aby odpovídaly existující databázi a všem lokálním konvencím pojmenování, a to tak, že budete postupovat podle postupu popsaného v komentářích na začátku souboru.

Důležité: Použijte online zařízení jako **SPUFI** ke spuštění příkazů, protože v souboru jsou komentáře a dávkové programy, jako je **DSNTINAD** , nepřijímají komentáře.

Spuštění úlohy modulu protokolování

Přejmenujte, přezkoumejte a odešlete člen BFGLGST Měli byste získat zprávu BFGDB0023I: Modul protokolování dokončil spouštěcí aktivity a je nyní spuštěn.

Operace modulu protokolování

Chcete-li zobrazit stav modulu protokolování, Přejmenovat, přezkoumat a odeslat člena BFGLGSH

Chcete-li zastavit modul protokolování, přejmenujte jej na člen BFGLGSP a odešlete jej.

z/OS Proměnné prostředí pro MFT v systému z/OS

Pokud spouštíte příkazy přímo z prostředí USS nebo vlastní skripty JCL, po přizpůsobení a konfiguraci musíte nastavit počet proměnných prostředí před spuštěním konfiguračních skriptů a skriptů administrace poskytnutých produktem Managed File Transfer. Tyto proměnné je třeba nastavit pro každého uživatele a pro každé prostředí, ze kterého budou skripty vyvolány.

Chcete-li se vyhnout konfliktům s jinými produkty, můžete se rozhodnout vytvořit skript `.wmqfterc` ve svém domovském adresáři. Skript `.wmqfterc` se pak vyvolá každým ze skriptů Managed File Transfer a tento skript můžete použít k poskytnutí vlastních nastavení prostředí pro produkt Managed File Transfer.

Existuje také jedna volitelná proměnná prostředí, BFG_WTO, kterou můžete nastavit pro odesílání zpráv do protokolu obsluhy při spouštění agentů z JCL.

Tabulka 49. Požadované proměnné prostředí z/OS

Proměnná prostředí	**Hodnota**
DOMOVSKÁ STRÁNKA BFG_JAVA_HOME	Umístění instalace produktu Java . Další informace o podporovaných úrovních Java naleznete v tématu Systémové požadavky pro IBM MQ.
BFG_DATA	Umístění datového adresáře pro Managed File Transfer for z/OS. Jedná se o cestu k produktu *DATA_DIR*.
STEPLIB	Musí obsahovat následující datové sady produktu IBM MQ : • SCSQAUTH • SCSQANLE • SCQLOAD Chcete-li spustit komponentu modulu pro protokolování databáze v systému z/OS , položka STEPLIB musí také obsahovat následující datové sady produktu Db2 v uvedeném pořadí: • SDSNANEXIT • SDSNLOD2 • SDSNLOAD

Tabulka 49. Požadované proměnné prostředí z/OS (pokračování)	
Proměnná prostředí	**Hodnota**
LIBPATH	Musí obsahovat umístění vašich knihoven produktu IBM MQJava v prostoru z/OS UNIX System Services (pro produkt IBM MQ 8.0je výchozí hodnota `/mqm/V8R0M0/java/lib`).

Dále je uveden příklad `.profile` , který správně konfiguruje proměnné prostředí pro Managed File Transfer:

```
LIBPATH=/mqm/V8R0M0/java/lib:$LIBPATH
STEPLIB=MQM.V800.SCSQAUTH:MQM.V800.SCSQANLE:MQM.V800.SCSQLOAD
PATH=/u/fteuser/bin:/u/fteuser/J7.0/bin:/bin:/usr/bin:/u/fteuser/extras/bin:/bin:$PATH
BFG_JAVA_HOME=/u/fteuser/J7.0
BFG_DATA=/u/fteuser/DATA_DIR
export PATH LIBPATH STEPLIB BFG_JAVA_HOME BFG_DATA
```

Volitelně můžete také nastavit následující proměnné prostředí:

Tabulka 50. Volitelná proměnná prostředí z/OS	
Proměnná prostředí	**Hodnota**
BFG_WTO	Jedna z následujících hodnot umožní společnosti BFG_WTO: • YES • ZAP • PRAVDA Jedna z následujících hodnot zakáže BFG_WTO. Tyto hodnoty nerozlišují velikost písmen. • NULL • NO • OFF • NEPRAVDA Povolí protokolování produktu z/OS . Při výchozím nastavení je tato proměnná prostředí zakázána. Zprávy, které jsou zapsány do protokolu událostí agenta, jsou také zapsány do protokolovacího zařízení z/OS obsluhy, které umožňuje snadnější přístup k automatizovaným produktům při spuštění agenta z JCL. Směrovací kód je Programmer Information (11) a kód deskriptoru je Informační (12).

Tabulka 50. Volitelná proměnná prostředí z/OS (pokračování)	
Proměnná prostředí	**Hodnota**
NÁZEV_SKUPINY_BFS	Skupina souborů `mqm` je obvykle asociována s konfiguračními datovými soubory a příkazy konfigurace produktu Managed File Transfer . V důsledku toho mohou všichni uživatelé, kteří jsou členy skupiny `mqm` , mít přístup a provádět změny v konfiguraci produktu Managed File Transfer . Další informace naleznete v tématu Oprávnění systému souborů pro MFT v IBM MQ. Pro systém z/OS je skupina souborů entitou systému souborů USS a skupina souborů `mqm` nemusí být nutně definována. Můžete definovat alternativní, existující skupinu systémů souborů z/OS USS pro konfigurační datové soubory produktu Managed File Transfer pomocí proměnné prostředí BFG_GROUP_NAME. Například na příkazovém řádku shellu USS: `export BFG_GROUP_NAME=FTEGB` který definuje skupinu FTEGB, která má být přidružena k jakýmkoli následně vytvořeným konfiguračním souborům pro aktuální relaci USS. Hodnotu BFG_GROUP_NAME můžete nastavit na prázdnou hodnotu, nebo ji můžete odebrat. Spustíte-li příkaz **`fteMigrateAgent`** na systému z/OS s proměnnou prostředí BFG_GROUP_NAME nastavenou na neprázdnou hodnotu, příkaz zkontroluje, zda je uživatel členem skupiny pojmenované proměnnou BFG_GROUP_NAME. Není-li uživatel členem pojmenované skupiny, může příkaz nahlásit chybovou zprávu `BFGCL0502E: Nemáte oprávnění k provedení požadované operace.` a nespustí se. Podrobné informace o kritériích, které musí uživatel splnit, aby úspěšně spustil tento příkaz, naleznete v tématu fteMigrateAgent .

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 produktu MFT pro produkt z/OS Automatic Restart Manager (ARM)

Managed File Transfer je aplikace s povoleným ARM.

Než začnete

Další informace o povolení ARM a definování zásad ARM pro váš systém najdete v tématu Použití správce automatického restartu z/OS (ARM).

Chcete-li použít schopnost protokolování produktu MFT Logger pro automatické restartování a opětovné připojení k databázi Db2 , ARM je jediným podporovaným správcem restartování, který je k dispozici.

Informace o této úloze

Použití ARM, agentů a zapisovačů protokolu lze nakonfigurovat pro restart nastavením vlastností agenta/modulu protokolování armELEMTYPEa armELEMENT. Vlastnost armELEMTYPE definuje typ prvku ARM a vlastnost armELEMENT je název prvku, který ARM má registrovat:

- Můžete nastavit typ agenta ELEMTYPE na SYSBFGAG a armELEMENT můžete nastavit tak, aby odpovídalo názvu agenta.
- Můžete nastavit modul protokolování ELEMTYPE na SYSBFGLG a armELEMENT lze nastavit tak, aby odpovídal názvu registrátoru.

Poznámka: Agenty a zapisovače protokolu, které jsou nakonfigurované pro restartování pomocí ARM, mohou být úspěšně spuštěny pouze z dávkové úlohy nebo spuštěné úlohy. Pokusy o spuštění agenta nebo zapisovače protokolu z příkazového řádku USS přímo selžou s kódem příčiny chyby ARM.

Příklad

Následující příklad zásady restartování definuje agenta BFGFT7CAG1 jako závislou osobu ve 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 skriptu JCL pro agenty Managed File Transfer na systému z/OS

Pomocí těchto informací můžete vygenerovat kód JCL, který lze použít k vytvoření a spuštění agenta v systému IBM MQ for z/OS.

Kopírovat ukázkovou knihovnu

Proveďte následující postup:

1. Vytvořte kopii knihovny SBFGCMDS (viz “Kopírovat SBFGCMDS pro vytvoření knihovny JCL” na stránce 661) otevřením knihovny.

   Většina členů, které začínají řetězcem BFGX, BFGY nebo BFGZ, jsou šablony, které používáte ke generování upraveného jazyka JCL pro agenta později.

   Důležitým členem je BFGCOPY.
2. Otevřít BFGCOPY a nahradit:

+ + suplepled_library + +
s názvem knihovny SBFGCMDS, která byla nainstalována jako součást produktu.

+ + servisní knihovna + +
jménem knihovny, kterou chcete použít pro svého agenta (cílovou knihovnu).

3. Odešlete úlohu a budete mít novou knihovnu, kterou můžete použít.

Upravit BFGCUSTM

Proveďte následující postup:

1. Otevřete novou knihovnu, abyste mohli upravit člen BFGCUSTM (viz "Úprava členu BFGCUSTM" na stránce 661)
2. Upravte všechny parametry v členu, které jsou uzavřeny uvnitř ++ znaků, a nahraďte je odpovídajícími hodnotami. Změňte například:

   + + bfg_prod + +
   Chcete-li ukázat na adresář USS, kde byl nainstalován produkt IBM MQ Managed File Transfer for z/OS .

   + + bfg_data + +
   Chcete-li být adresářem USS, kde má být uložena vaše konfigurace produktu IBM MQ Managed File Transfer for z/OS .

   + + typ_služby + +
   Do slova AGENT

   + + název_agenta + +
   Název vašeho agenta

Notes:

1. Některé položky, jako např. `++options++` požadované pro CLEAN_AGENT_PROPS, nejsou potřebné, a proto byste je měli odstranit.
2. See "Než začnete" na stránce 656 for a complete list of all of the parameters in the BFGCUSTM member, along with a description of what values they should have.

Odešlete soubor JCL BFGCUSTM

Proveďte následující postup:

1. Odešlete úlohu.
2. Ukončete knihovnu v ISPF.

   To je nezbytné, protože úloha BFGCUSTM aktualizuje knihovnu a nemůže ji dělat, když je knihovna otevřená.
3. Když se úloha dokončí, podívejte se do protokolu úlohy.

   Zobrazí se počet zpráv, které označují, že v knihovně byly vytvořeny nové členy.

   Každý z těchto členů obsahuje JCL, které lze použít k provádění specifických úloh pro vašeho agenta. Seznam těchto členů naleznete v části "z/OS skripty JCL příkazů agenta a modulu protokolování" na stránce 670 spolu s příkazy IBM MQ Managed File Transfer , které odpovídají.

Odeslat BFGAGCR k vytvoření agenta

Nový člen BFGAGCR obsahuje kód JCL, který vytvoří agenta vyvoláním příkazu **`fteCreateAgent`** .

Proveďte následující postup:

1. Otevřete člen BFGAGCR.

   Měli byste vidět, že BFGAGCR byl naplněn názvem vašeho:

   - Agent

- Správce front agenta
- Koordinační správce front pro topologii produktu MFT

2. Odešlete člen BFGAGCR.

   Je-li člen spuštěn, postupujte takto:

   - Vytvoří požadované konfigurační soubory pro vašeho agenta.
   - Připojí se ke správci front agenta a vytvoří systémové fronty, které agent potřebuje, pomocí CSQUTIL.
   - Registruje agenta s koordinačním správcem front.

Spusťte agenta odesláním BFGAGST

Proveďte následující postup:

1. Odešlete člena BFGAGST. Viz použití agenta pro různé příkazy, které ukazují, že agent pracuje správně.
2. Když je úloha dokončena, 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, běží a je připraven na provedení spravovaných přenosů.

z/OS Přesun agenta MFT do nové logické oblasti z/OS

Někdy je nezbytné přesunout agenta IBM MQ Managed File Transfer for z/OS z jedné logické oblasti do jiné a zároveň udržet agenta ve stejné topologii produktu IBM MQ Managed File Transfer se stejnou koordinací a správci front příkazů. Kroky potřebné k provedení této akce závisejí na tom, jak byl migrovaný agent původně vytvořen.

Informace o této úloze

Přesuňte svého agenta IBM MQ Managed File Transfer for z/OS jedním z následujících způsobů:

- Pokud byl agent původně vytvořen pomocí vlastní verze knihovny SBFGCMCMDS, použijte knihovnu k novému vytvoření v nové logické oblasti.
- Pokud byl agent původně vytvořen spuštěním příkazů USS, použijte příkazy k jeho opětovnému vytvoření v nové oblasti LPAR.

Poznámka:

Naplánované přenosy a přenosové šablony jsou uloženy v koordinačním správci front pro topologii produktu IBM MQ Managed File Transfer . Tato úloha předpokládá, že koordinační správce front není součástí přesunu práce. V takovém případě zůstanou všechny naplánované přenosy a šablony přenosu přidružené k přesouvaných agentovi po dokončení přesunu ve správci front pro stávající koordinaci zachovány.

Procedura

- Přesuňte agenta vytvořeného pomocí přizpůsobené verze knihovny SBFGCMCMDS.

  Pokud byl agent vytvořen pomocí upravené verze knihovny SBFGCMCMDS, můžete použít tuto knihovnu k opětovnému vytvoření prostředí IBM MQ Managed File Transfer for z/OS a konfiguraci agenta na nové oblasti LPAR. Postupujte takto:

  1. Zkopírujte upravenou verzi knihovny z původní oblasti LPAR do nové oblasti LPAR.
  2. Upravte člen BFGCUSTM v přizpůsobené verzi knihovny v nové oblasti LPAR a ujistěte se, že hodnoty parametrů jsou stále platné.
  3. Spusťte člen BFGCUSTM v nové oblasti LPAR, chcete-li vytvořit všechny JCL potřebné ke konfiguraci prostředí a k vytvoření agenta.

4. Spuštěním členu BFGCFCR definujte koordinačního správce front, který má být použit agentem v nové oblasti LPAR, a vytvořte adresářovou strukturu potřebnou k uložení konfigurace produktu IBM MQ Managed File Transfer .
5. Dále spusťte člen BFGCMCR, chcete-li definovat správce front příkazů, který má použít agent na nové oblasti LPAR.
6. Chcete-li znovu vytvořit agenta a jeho konfiguraci, spusťte člen BFGAGCR.
7. Ujistěte se, že systémové fronty použité agentem existují na správci front pro tohoto agenta.

Pokud má přesouvaná agent přidružené monitory prostředků, musíte znovu vytvořit monitory na novém agentovi. Postupujte takto:

1. V původní logické oblasti spusťte člen BFGMNLI a exportujte definice pro monitor prostředků přidružený k původnímu agentovi do souborů XML.
2. Zkopírujte soubory XML obsahující definice monitoru prostředků do nové oblasti LPAR.
3. Chcete-li importovat definice monitoru prostředků uložené v souborech XML, použijte člen BFGMNCRS v knihovně SBFGCMCMDS v nové oblasti LPAR. To má za následek vytvoření monitorů na novém agentovi.

- Přesuňte agenta vytvořeného spuštěním příkazů v prostředí USS.

  Pokud byl agent původně vytvořen spuštěním příkazů USS, můžete použít příkazy k novému vytvoření agenta v nové oblasti LPAR. Postupujte takto:

  1. Spusťte příkaz fteSetupCoordination v nové oblasti LPAR, definujte koordinačního správce front, který má být používán agentem, a vytvořte adresářovou strukturu potřebnou k uložení konfigurace produktu IBM MQ Managed File Transfer .
  2. Spuštěním příkazu fteSetupCommands definujte správce front příkazů, který má být použit agentem v nové oblasti LPAR.
  3. Spusťte příkaz fteCreateAgent , abyste znovu vytvořili agenta a jeho konfiguraci.
  4. Ujistěte se, že systémové fronty použité agentem existují na správci front pro tohoto agenta.

  Pokud má přesouvaná agent přidružené monitory prostředků, musíte znovu vytvořit monitory na novém agentovi. Postupujte takto:

  1. V původní logické oblasti spusťte příkaz fteListMonitors a uveďte parametr **-ox** , chcete-li exportovat definice pro monitor prostředků přidružený 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 zadáním parametru **-ix** , který importuje definice monitoru prostředků uložené v souborech XML. To má za následek vytvoření monitorů na novém agentovi.

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 ve svém systému IBM MQ for z/OS .

Přehled

Produkt Managed File Transfer for z/OS (MFT) používá standardní instalační proceduru produktu z/OS . Alternativním způsobem spouštění příkazů produktu MFT je použití JCL a spouštěcího programu JZOS Java Launcher.

Další podrobnosti viz Spouštěcí program dávky JZOS a sada nástrojů Toolkit .

Pokud se vaše JCL nedaří správně zpracovat, prohlédněte si téma Problémy běžného MFT s JZOS.

Příklad souboru JCL pro produkt IBM MQ 8.0 a novější

Upozornění: Pro IBM WebSphere MQ File Transfer Edition 7.0začínají parametry řetězcem FTE_ místo BFG_.

```
//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 určeného člena JCL z umístění v 1)
- (2A) To rozšiřuje // STDENV-viz níže
- (3) To je příkaz, který má být proveden, bez úvodní předpony fte
- (4) Tyto řádky jsou nezbytné, nastavují informace pro JZOS
- (5) Parametry příkazu
- Člen BFGJCL8 (můžete vybrat své vlastní jméno) vyvolá JZOS. Tento člen má k dispozici STEPLIB a další JCL potřebné ke spuštění produktu MFT.

Další jazyk JCL, který je třeba zahrnout

Měli byste zahrnout JCL pro knihovny IBM MQ for z/OS a pokud používáte registrátor 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.V800.SCSQAUTH,DISP=SHR MQ Bindings
//   DD DSN=MQM.V800.SCSQANLE,DISP=SHR MQ Bindings
//   DD DSN=MQM.V800.SCSQLOAD,DISP=SHR MQ Bindings

//* DB2 libraries
//   DD DISP=SHR,DSN=SYS2.DB2.V10.SDSNEXIT.DBCP
//   DD DISP=SHR,DSN=SYS2.DB2.V10.SDSNLOAD
//   DD DISP=SHR,DSN=SYS2.DB2.V10.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. Podívejte se do souboru SYS1.SIEALNKE pro verzi na vašem systému. Přidejte, PARM = '+ T', abyste získali další diagnostiku.
- (2) Jedná se o datovou sadu s programem JZOS.
- (3) Jedná se o název člena skriptu shellu. Definuje parametry potřebné pro MFT. Viz téma “Skript shellu pro definování MFT” na stránce 683.

  Může se jednat o libovolnou datovou sadu a člena. Je třeba, aby byla v souboru naposledy, protože úloha JCL je rozšířením této úlohy. Viz 2A v příručce “Příklad souboru JCL pro produkt IBM MQ 8.0 a novější” na stránce 682.

Skript shellu pro definování MFT

V příkladu “Další jazyk JCL, který je třeba zahrnout” na stránce 682 se použije člen BFGZENV8 . To je založeno na profilu JZOS.

Pro produkt MFT V8 a IBM WebSphere MQ File Transfer Edition 7.0můžete použít stejný konfigurační soubor, přičemž některé menší změny se změní. Nezapomeňte, že před verzí MFT V8 parametry začínají na FTE. Viz téma “Ukázkový soubor” na stránce 683.

Musíte vědět:

- Umístění, kde je nainstalován produkt Java .
- Umístění knihoven produktu IBM MQ for z/OS Java
- Umístění souborů MFT
- ID uživatele musí být ve specifické skupině, aby bylo považováno za administrátora produktu IBM MQ for z/OS . Potřebujete název této skupiny
- Pokud pro zprávy nepoužíváte angličtinu, musíte vědět, který jazyk chcete uvést.

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/V8R0M0/java/lib/"
export LIBPATH

export BFG_JAVA_HOME="${JAVA_HOME}"
export BFG_WTO="YES"
export BFG_GROUP_NAME=MQADM
export BFG_PROD="/HMF8800/"
export BFG_CONFIG="/u/johndoe/fteconfig"
# export BFG_LANG=" -Duser.language=de "
export BFG_LANG=" "

--------------------
```

kde:

export _BPXK_AUTOCVT = "ON "
Je požadován pro kódování Unicode

export JAVA_HOME = "/java/java71_bit64/J7.1_64/"
Jedná se o umístění adresáře Java. Uveďte název cesty pro Java. Tento adresář obsahuje bin a další adresáře.

export PATH= "/bin: ${JAVA_HOME}/bin/classic/"
Nastaví příkaz cesty pro spustitelné příkazy jazyka Java

LIBPATH= "/lib:/usr/lib:${JAVA_HOME}/bin"
Nastaví cestu ke knihovně pro spustitelné příkazy Java

LIBPATH=" $LIBPATH: ${JAVA_HOME}/bin/classic"
Přidává více knihoven Java do příkazu LIBPATH.

LIBPATH=$LIBPATH: "/mqm/V8R0M0/java/lib/"
Přidá knihovny IBM MQ for z/OS do cesty ke knihovně. Zadejte název svých knihoven IBM MQ for z/OS v prostředí USS.

export LIBPATH
Zpřístupní LIBPATH pro JZOS

export BFG_JAVA_HOME = "${JAVA_HOME}"
Nastaví hodnotu parametru BFG_JAVA_HOME na hodnotu proměnné JAVA_HOME zadané výše.

export BFG_WTO = "YES "
Nastavení BFG_WTO na YES způsobí, že se zprávy budou zobrazovat v protokolu úlohy pomocí WTO

export BFG_GROUP_NAME=MQADM
Identifikátory uživatele, které jsou členy uvedené skupiny, jsou považovány za administrátory produktu IBM MQ for z/OS .

export BFG_PROD = "/HMF8800/"
Jedná se o cestu, kde je umístěn kód MFT

export BFG_DATA= "/u/johndoe/ftecconfig"
Je místo, kde jsou uloženy informace o konfiguraci MFT

 # export BFG_LANG = " -Duser.language= de"
Je komentář k definici jazyka jako němčinu, který je označen jako komentář

export BFG_LANG = ""
Určuje jazyk jako výchozí jazyk v angličtině.

Obsah produktu MFT v produktu `/lib/messages/BFGNVMessages_*.properties` uvádí seznam jazyků, které jsou k dispozici. Výchozím nastavením je ponechat hodnotu prázdnou, což znamená, že se použije angličtina.

Pro V7 zadejte:

```
export FTE_JAVA_HOME="${JAVA_HOME}"
export FTE_WTO="YES"
export FTE_GROUP_NAME=SCENU
export FTE_PROD=""/HMF7100/"
export FTE_CONFIG="/u/johndoe/fteconfig"
export BFG_LANG=" "
```

Všimněte si, že `/u/johndoe/fteconfig` se liší od serveru v souboru BFG_DATA

Související úlohy

“Konfigurace produktu Managed File Transfer for z/OS” na stránce 655
Produkt Managed File Transfer for z/OS vyžaduje přizpůsobení, aby mohla komponenta pracovat správně.

Plánování pro databázi Managed File Transfer

IBM i Konfigurace produktu MFT v systému IBM i

Chcete-li začít používat produkt Managed File Transfer poté, co jste jej nainstalovali, musíte dokončit konfiguraci pro koordinačního správce front a agenta.

Informace o této úloze

Po instalaci musíte spustit konfigurační skripty poskytnuté produktem Managed File Transfer pro nové koordinační správce front a nové agenty předtím, než budete moci používat koordinační správce front a agenty k přenosu souborů. Pak 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 koordinační správce front není na stejném počítači jako instalace, zkopírujte skriptový soubor MQSC na počítač, kde je umístěn správce front, a poté spusťte skript.

   a) Z příkazového řádku IBM i spusťte příkaz qshell pomocí následujícího příkazu: `CALL QSHELL`

b) Přejděte do následujícího adresáře: /QIBM/UserData/mqm/mqft/config/*coordination_qmgr_name*

c) Vydejte následující příkaz a nahraďte hodnotu *coordination_qmgr_name* názvem svého správce front:

```
/QSYS.LIB/QMQM.LIB/RUNMQSC.PGM coordination_qmgr_name < coordination_qmgr_name.mqsc
```

Koordinačního správce front můžete namísto toho nakonfigurovat ručně. Další informace viz téma “Konfigurace koordinačního správce front pro produkt MFT” na stránce 688.

2. Pro všechny nové agenty: spusťte příkazy MQSC v souboru *agent_name*_create.mqsc pro správce front agenta.

   Pokud se správce front agenta nenachází na stejném počítači jako agent, zkopírujte skriptový soubor MQSC na počítač, kde je správce front umístěn, a poté spusťte skript.

   a) Z příkazového řádku IBM i spusťte příkaz qshell pomocí následujícího příkazu: CALL QSHELL

   b) Přejděte do následujícího adresáře: /QIBM/UserData/mqm/mqft/config/*agent_qmgr_name*/agents

   c) Vydejte následující příkaz, nahraďte *agent_qmgr_name* názvem svého správce front agenta a nahradíte *název_agenta* názvem vašeho agenta:

```
/QSYS.LIB/QMQM.LIB/RUNMQSC.PGM agent_qmgr_name < agent_name_create.mqsc
```

   Správce front agenta můžete místo něj nakonfigurovat ručně. Další informace viz “Konfigurace správců front agenta MFT” na stránce 688.

3. Pokud jste již 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 IBM i spusťte příkaz qshell pomocí následujícího příkazu: CALL QSHELL

   b) Přejděte do následujícího adresáře: /QIBM/ProdData/mqm/bin

   c) Vydejte následující příkaz a nahraďte AGENT názvem vašeho 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 pískovišti agenta MFT.

Související pojmy

“Konfigurace produktu MFT pro první použití” na stránce 685
Musíte provést některé konfigurační úlohy pro agenty Managed File Transfer a správce front jednou, a to poprvé, kdy je chcete použít.

Konfigurace produktu MFT pro první použití

Musíte provést některé konfigurační úlohy pro agenty Managed File Transfer a správce front jednou, a to poprvé, kdy je chcete použít.

připojeníIBM MQ

Veškerá síťová komunikace se správci front produktu IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály produktu IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo kanály MQI.

Managed File Transfer a kanály

Produkt Managed File Transfer používá kanály MQI k připojení agentů v režimu klienta ke správcům front agenta a k připojení aplikací příkazů (například **fteCreateTransfer**) k jejich příkazům a koordinačním správcům front. Ve výchozí konfiguraci jsou tato připojení prováděna pomocí kanálu SVRCONN s názvem SYSTEM.DEF.SVRCONN, který ve všech správcích front standardně existuje. Vzhledem k těmto výchozím nastavením není třeba měnit žádné kanály MQI pro základní instalaci produktu Managed File Transfer .

Existuje šest typů koncových bodů kanálu zpráv, ale toto téma pokrývá pouze dvojice odesilatel-příjemce. Informace o dalších kombinacích kanálů najdete v tématu Distribuované komponenty řazení do fronty .

Požadované cesty ke zprávám

Zprávy produktu IBM MQ mohou cestovat pouze kanály zpráv, takže je třeba zajistit, aby kanály byly dostupné pro všechny cesty zpráv vyžadované produktem Managed File Transfer. Tyto cesty nemusí být přímé; zprávy mohou v případě potřeby cestovat zprostředkujícími správci front. Toto téma pojednává pouze o přímé dvoubodové komunikaci. Další informace o těchto volbách najdete v tématu Jak se dostat ke vzdálenému správci front .

Komunikační cesty používané produktem Managed File Transfer jsou následující:

Agent k agentovi
: Všechny dva agenty, které jsou přenášené soubory, vyžadují obousměrnou komunikaci mezi jejich přidruženými správci front. Vzhledem k tomu, že tato cesta obsahuje hromadná data, zvažte co možná nejkratší cestu podle vašich potřeb, jak je to možné, co nejrychleji.

Agent pro koordinaci
: Protokolovat zprávy od agentů, kteří se účastní přenosu, musí být schopni se dostat ke koordinačnímu správci front.

Příkaz k agentovi
: Jakýkoli správce front, který se používá k příkazům aplikací nebo IBM MQ Explorer (pomocí správce front příkazů), musí být schopen odesílat zprávy správcům front agentů, kteří tyto příkazové aplikace používají ke kontrole. Chcete-li povolit příkazy zpětné vazby, které mají být zobrazeny v příkazech, použijte obousměrné připojení.

Další informace naleznete v tématu *Ověření instalace produktu IBM MQ* pro platformu nebo platformy, kterou váš podnik používá.

Související pojmy

“Konfigurace správce front s více instancemi pro práci s produktem MFT” na stránce 692
IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front s více instancemi se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agentů s více instancemi, koordinačním správcem front s více instancemi a správci front s více instancemi.

Související úlohy

“Konfigurace správců síťových front produktu MFT” na stránce 686
Pokud vaše síť produktu Managed File Transfer obsahuje více než jednoho správce front IBM MQ , musí být tito správci front produktu IBM MQ schopni vzdáleně komunikovat.

“Konfigurace koordinačního správce front pro produkt MFT” na stránce 688
Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* a proveďte nezbytnou konfiguraci pro koordinačního správce front. Pokud však chcete tuto konfiguraci provést ručně, proveďte na koordinačním správci front následující kroky.

Konfigurace správců síťových front produktu MFT

Pokud vaše síť produktu Managed File Transfer obsahuje více než jednoho správce front IBM MQ , musí být tito správci front produktu IBM MQ schopni vzdáleně komunikovat.

Informace o této úloze

Existují dva způsoby, jak nakonfigurovat správce front tak, aby mohli komunikovat mezi sebou navzájem:

- Nastavením klastru správce front produktu IBM MQ .

  Informace o klastrech správců front IBM MQ a o tom, jak je konfigurovat, viz “Konfigurace klastru správce front” na stránce 265.
- Nastavením kanálů mezi správci front, který je popsán následujícím způsobem:

Nastavení kanálů mezi správci front

Nastavte následující kanály zpráv mezi správci front:

- Ze správce front agenta do koordinačního správce front
- Ze správce front příkazů na správce front agenta.
- Ze správce front agenta do správce front příkazů (chcete-li povolit zobrazení 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

Pokud potřebujete další informace o tom, jak nastavit tuto komunikaci, začněte s touto informací: Administrace vzdálených objektů IBM MQ pomocí MQSC.

Některé navrhované vzorové kroky jsou:

Postup

1. Vytvořte přenosovou frontu ve správci front produktu IBM MQ se stejným názvem jako koordinačního správce front.

   Můžete použít následující příkaz MQSC:

   ```
   DEFINE QLOCAL(coordination-qmgr-name) USAGE(XMITQ)
   ```
2. Ve správci front produktu IBM MQ vytvořte odesílací kanál pro koordinačního správce front produktu Managed File Transfer . Název přenosové fronty vytvořené v předchozím kroku je povinný parametr pro tento kanál. Je-li vyžadována komunikace s agenty Managed File Transfer for IBM WebSphere MQ 7.5 nebo Managed File Transfer , ujistěte se, že parametr CONVERT kanálu odesílatele je nastaven na hodnotu no. (Starší verze produktu IBM WebSphere MQ File Transfer Edition vždy publikují zprávy ve formátu UTF-8 , což znamená, že jakákoli konverze dat poškodí zprávu. To není nezbytné pro agenty na serveru Managed File Transfer pro produkt IBM MQ 8.0 nebo pozdější, protože zprávy jsou 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 CONVERT (NO), pouze je-li to požadováno.
3. V koordinačním správci front produktu Managed File Transfer vytvořte přijímací kanál pro správce front produktu IBM MQ . Udělit tomuto přijímacímu kanálu stejný název jako odesílací kanál ve správci front IBM MQ .

   Můžete použít následující příkaz MQSC:

   ```
   DEFINE CHANNEL(channel-name) CHLTYPE(RCVR)
   ```

Jak pokračovat dále

Dále postupujte podle kroků konfigurace pro koordinačního správce front: “Konfigurace koordinačního správce front pro produkt MFT” na stránce 688.

Konfigurace koordinačního správce front pro produkt MFT

Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* a proveďte nezbytnou konfiguraci pro koordinačního správce front. Pokud však chcete tuto konfiguraci provést ručně, proveďte na koordinačním správci front následující kroky.

Informace o této úloze

Postup

1. Vytvořte lokální frontu s názvem SYSTEM.FTE.
2. Přidejte SYSTEM.FTE fronta na SYSTEM.QPUBSUB.QUEUE.NAMELIST seznam názvů.
3. Vytvořte téma s názvem SYSTEM.FTE s řetězcem tématu SYSTEM.FTE.
4. Ujistěte se, že atributy NPMSGDLV (Non-persistent Message delivery) a PMSGDLV (Persistent Message delivery) v SYSTEM.FTE je nastaven na hodnotu ALLAVAIL.
5. Ujistěte se, že je atribut režimu publikování/odběru (PSMODE) koordinačního správce front nastaven na hodnotu ENABLED.

Jak pokračovat dále

Pokud spustíte příkaz `strmqm -c` ve správci front, který byl konfigurován jako koordinační správce front, odstraní tento příkaz změnu provedená v kroku 2 (přidání SYSTEM.FTE fronta na SYSTEM.QPUBSUB.QUEUE.NAMELIST seznam názvů). Důvodem je to, že `strmqm -c` znovu vytvoří výchozí objekty IBM MQ a vrátí změny Managed File Transfer . Pokud jste tedy spustili správce front s produktem `strmqm -c`, proveďte jeden z následujících kroků:

- Znovu spusťte skript *coordination_qmgr_name*.mqsc ve správci front.
- Zopakujte krok 2.

Související pojmy

“připojeníIBM MQ” na stránce 685
Veškerá síťová komunikace se správci front produktu IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály produktu IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo kanály MQI.

“Konfigurace správce front s více instancemi pro práci s produktem MFT” na stránce 692
IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front s více instancemi se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agentů s více instancemi, koordinačním správcem front s více instancemi a správci front s více instancemi.

Související úlohy

“Konfigurace správců síťových front produktu MFT” na stránce 686
Pokud vaše síť produktu Managed File Transfer obsahuje více než jednoho správce front IBM MQ , musí být tito správci front produktu IBM MQ schopni vzdáleně komunikovat.

Související odkazy

fteSetup-koordinace

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* , abyste provedli nezbytnou konfiguraci pro správce

front agenta. Pokud však chcete provést tuto konfiguraci ručně, proveďte tyto kroky na 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*

   Další informace o parametrech fronty naleznete v tématu Nastavení fronty agenta produktuMFT.
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*

   Další informace o parametrech fronty naleznete v tématu Nastavení fronty agenta produktuMFT.

Jak pokračovat dále

Informace o vytvoření a konfiguraci agenta mostu protokolu viz fteCreateBridgeAgent (vytvoření a konfigurace agenta mostu protokolu MFT) a Konfigurace mostu protokolů pro server FTPS.

Vytvoření struktury přenosu souborů IBM MQ

Strukturu produktu Managed File Transfer můžete nakonfigurovat na základě jediného agenta připojeného ke správci front na stejném počítači.

Informace o této úloze

Konfigurace produktu MFT je uložena ve struktuře souborů pod položkou IBM MQ DataPathna počítači, na kterém bude agent umístěn.

Následující ukázka konfigurace je pro produkt MFT se správcem front IBM MQ 8.0 s názvem SAMPLECOORD (se zakázaným zabezpečením) a jediným agentem 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 vypnuto. Následující příkazy spuštěné v produktu **runmqsc**budou po restartování správce front znepřístupnit zabezpečení:

```
runmqsc queue manager
 alter qmgr CONNAUTH(NONE);
 alter qmgr CHLAUTH(DISABLED);
 end;
```

Pro konfiguraci s povoleným zabezpečením v produktu MFT pro produkt IBM MQ 8.0 nebo novější produkt **CONNAUTH** vyžaduje všechny příkazy produktu MFT , které se připojují ke správci front, kvůli zadání pověření ID uživatele a hesla. Pro každý příkaz můžete použít dodatečné parametry **-mquserid** a **-mqpassword** , nebo můžete definovat soubor `MQMFTCredentials.xml` . Následující ukázka souboru pověření definuje ID uživatele produktu `fteuser`, pro které má být použito heslo produktu `MyPassword` při připojování 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 téma Ověření připojeníMFT a IBM MQ.

Notes:

- Chcete-li vyhledat konfigurační adresář produktu MFT , použijte příkaz **fteDisplayVersion -v** .
- Pro uživatele produktu z/OS může být soubor `MQMFTCredential.xml` umístěn jako člen v rozdělené datové sadě s proměnlivým formátem záznamu (RECFM = V) nebo nedefinovaným formátem záznamu (RECFM = U).
- Pro konfiguraci s povoleným zabezpečením přidejte následující parametr do níže uvedených kroků, chcete-li přidružit pověření k příslušnému správci front: `-credentialsFile` *full credential file path*.
- Heslo pro nečitelné textové heslo v produktu `MQMFTCredential.xml` lze zamlžit pomocí následujícího příkazu:

  ```
  fteObfuscate -credentialsFile full file path to MQMFTCredentials.xml
  ```

Postup

1. Vytvořte koordinačního správce front.

   Koordinační správce front je jedním správcem front, který se používá pro příjem všech informací o protokolu přenosu a informace o stavu od agentů. Spusťte tento příkaz:

   ```
   fteSetupCoordination -coordinationQMgr coordination_qmgr_name
   ```

   Tím se vytvoří základní konfigurace nejvyšší úrovně a vytvořte skriptový soubor IBM MQ pro volání *coordination_qmgr_name*`.mqsc`.

   Konfiguraci je pak nutné 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
```

U vytvořeného produktu *coordination_qmgr_name*.mqscbude třeba spustit příkaz **runmqsc** na stejném počítači, na kterém je spuštěn koordinační správce front.

2. Vytvořte správce front příkazů.

   Správce front příkazů je jedním správcem front, který byl předkonfigurován tak, aby infrastruktura IBM MQ mohla směrovat požadavky MFT na příslušného agenta. Spusťte tento příkaz:

   ```
   fteSetupCommands -connectionQMgr Command QM Name -p Coordination QM Name
   ```

   Tím se vytvoří soubor command.properties v koordinačním adresáři. Všimněte si, že -p je volitelný, a není požadován, 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 tento příkaz:

   ```
   fteCreateAgent -p coordination_qmgr_name -agentName agent_name -agentQMgr agent_qmgr_name
   ```

   Tím se vytvoří konfigurace agenta v rámci koordinace a vytvoří soubor skriptu 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 tento příkaz:

   ```
   fteStartAgent -p coordination_qmgr_name agentName
   ```

   Agent se spustí na pozadí a vrátí se příkazový řádek. Chcete-li zkontrolovat, zda je agent spuštěný, spusťte následující příkaz:

   ```
   fteListAgents -p coordination_qmgr_name
   ```

   Zobrazuje stav agentů. Je-li agent úspěšně spuštěn, bude ohlášen jako ve stavu PŘIPRAVENO.

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 moduly plug-in produktu MFT k vytváření a monitorování přenosů.

Více agentů lze přidat do konfigurace zopakováním kroku 3: Vytvoření agenta. Je-li použito připojení klienta TCP, mohou být použity na různých počítačích. U různých počítačů se musí příkazy

fteSetupCoordination a **fteSetupCommands** opakovat pro každý počítač, avšak skripty mqsc nebudou muset být spuštěny.

Složitější konfigurace mohou mít oddělené správce front pro koordinaci a každého agenta. V těchto případech budou muset být různí správci front připojeni společně.

Související úlohy

Co dělat, pokud váš agent MFT není vypsán příkazem **fteListAgents**

Související odkazy

fteSetup-koordinace

Příkazy fteSetup: Vytvoření souboru MFT command.properties

Agent fteCreate

fteObfuscate: šifrovat citlivá data

Formát souboru pověření MFT

Soubor MFTagent.properties

Konfigurace správce front s více instancemi pro práci s produktem MFT

IBM WebSphere MQ 7.0.1 dále podporuje vytváření správců front s více instancemi. Správce front s více instancemi se automaticky restartuje na záložním serveru. Produkt Managed File Transfer podporuje připojení ke správcům front agentů s více instancemi, koordinačním správcem front s více instancemi a správci front s více instancemi.

Konfigurace správce front s více instancemi

Důležité: Informace o konfiguraci správce front pro více instancí produktu IBM MQ naleznete v tématu “Správci front s více instancemi” na stránce 457. Před pokusem o konfiguraci správce front pro více instancí, který má pracovat s produktem Managed File Transfer, se ujistěte, že jste si přečetli tyto informace.

Použití správce front s více instancemi jako správce front agenta

Chcete-li povolit agenta, aby se mohl připojit k aktivní a záložní instanci vašeho správce front s více instancemi, 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, to znamená, že je *host_name*(*port_number*).

Vlastnost `agentQMgr` určuje název správce front s více instancemi. Vlastnost `agentQMgrHost` uvádí název hostitele pro aktivní instanci správce front a vlastnost `agentQMgrPort` uvádí číslo portu pro aktivní instanci správce front. Agent se musí připojit v režimu klienta k aktivní a záložní instanci správce front s více instancemi.

Další informace najdete v tématu Soubor MFT `agent.properties` .

Tento příklad ukazuje obsah souboru `agent.properties` pro AGENT1 , který se připojuje ke správci front s více instancemi s názvem QM_JUPITER. Aktivní instance správce front QM_JUPITER je v systému host1 a používá číslo portu 1414 pro připojení klienta. Rezervní instance správce front 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 záložní instanci koordinačního správce front s více instancemi, přidejte vlastnost `coordinationQMgrStandby` do všech souborů `coordination.properties` ve své topologii produktu Managed File Transfer .

Další informace najdete v tématu Soubor MFT coordination.properties .

Tento příklad ukazuje obsah souboru `coordination.properties` , který určuje podrobnosti připojení ke koordinačnímu správci front s více instancemi s názvem QM_SATURN. Aktivní instance správce front QM_SATURN je v systému coordination_host1 a používá číslo portu 1420 pro připojení klienta. Rezervní instance správce front 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 produktu Managed File Transfer se musí vždy připojit ke svému správci front v režimu vazeb. Při použití samostatného modulu protokolování s koordinačním správcem front s více instancemi se připojuje samostatný modul protokolování v režimu vazeb k jinému správci front. Kroky, které je třeba provést, jsou popsány v tématu “Alternativní konfigurace pro samostatný modul protokolování produktu MFT” na stránce 707. Je třeba definovat kanály mezi správcem front samostatného modulu protokolování a koordinačním správcem front s názvem hostitele a číslem portu obou instancí koordinačního správce front s více instancemi. Informace o tom, jak to provést, viz “Správci front s více instancemi” na stránce 457.

Modul plug-in produktu Managed File Transfer pro produkt IBM MQ Explorer se připojuje ke koordinačnímu správci front v režimu klienta. Pokud aktivní instance koordinačního správce front s více instancemi selže, stane se aktivní instance koordinačního správce front aktivním a znovu se připojí modul plug-in.

Příkazy Managed File Transfer **`fteList*`** a **`fteShowAgentDetails`** se připojují přímo ke koordinačnímu správci front. Je-li aktivní instance koordinace s více instancemi nedostupná, tyto příkazy se pokusí připojit k instanci v pohotovostním režimu koordinačního správce front.

Použití správce front s více instancemi jako správce front příkazů

Chcete-li povolit připojení k aktivní i záložní instanci správce front příkazů s více instancemi, přidejte vlastnost `connectionQMgrStandby` do všech souborů `command.properties` ve své topologii produktu Managed File Transfer .

Další informace viz Soubor MFT command.properties .

Tento příklad ukazuje obsah souboru `command.properties` , který určuje podrobnosti připojení pro správce front příkazů s více instancemi s názvem QM_MARS. Aktivní instance QM_MARS je na systému command_host1 a používá číslo portu 1424 pro připojení klienta. Rezervní 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 685
Veškerá síťová komunikace se správci front produktu IBM MQ , včetně komunikace související s produktem Managed File Transfer, zahrnuje kanály produktu IBM MQ . Kanál IBM MQ představuje jeden konec síťového propojení. Kanály jsou klasifikovány buď jako kanály zpráv, nebo kanály MQI.

Související úlohy

"Konfigurace správců síťových front produktu MFT" na stránce 686
Pokud vaše síť produktu Managed File Transfer obsahuje více než jednoho správce front IBM MQ , musí být tito správci front produktu IBM MQ schopni vzdáleně komunikovat.

"Konfigurace koordinačního správce front pro produkt MFT" na stránce 688
Po spuštění příkazu **fteSetupCoordination** spusťte skript *coordination_qmgr_name*.mqsc v adresáři *MQ_DATA_PATH*/mqft/config/*coordination_qmgr_name* a proveďte nezbytnou konfiguraci pro koordinačního správce front. Pokud však chcete tuto konfiguraci provést ručně, proveďte na koordinačním správci front následující kroky.

Uchování zpráv protokolu produktu 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 . Nejsou-li k dispozici žádné odběry, tyto informace se neuchovávají.

Způsoby zajištění zachování informací

Pokud jsou informace o průběhu přenosu nebo protokolu důležité pro vaše podnikání, je třeba provést jeden z následujících kroků, abyste se ujistili, že jsou informace zachovány:

- Použijte modul protokolování databáze produktu Managed File Transfer ke kopírování zpráv publikovaných do systému SYSTEM.FTE/Log se používá k databázi Oracle nebo Db2 .
- Definujte odběr pro SYSTEM.FTE téma, které ukládá publikace ve frontě produktu IBM MQ . Definujte tento odběr před přenosem jakýchkoli přenosů souboru, abyste se ujistili, že jsou ve frontě zachovány všechny zprávy o průběhu zpracování a zprávy protokolu.
- Napište aplikaci, která používá rozhraní MQI (Message Queue Interface) nebo produkt IBM MQ JMS k vytvoření trvalého odběru a zpracování publikací, které jsou doručovány do odběru. Tato aplikace musí být v činnosti před přenosem jakýchkoli souborů, aby se zajistilo, že aplikace obdrží všechny zprávy o průběhu a ve zprávách protokolu.

Každý z těchto přístupů je podrobněji popsán v následujících sekcích.

Nespoléhejte se na modul plug-in produktu IBM MQ Explorer , aby uchoval informace protokolu.

Použití modulu protokolování databáze produktu Managed File Transfer k uchování zpráv protokolu

Modul pro protokolování databáze je volitelná komponenta produktu Managed File Transfer , kterou lze použít ke kopírování informací z protokolů do databáze pro účely analýzy a auditu. Modul pro protokolování databáze je samostatná aplikace produktu Java , kterou instalujete v systému, který je hostitelem koordinačního správce front a databáze. Další informace o registrátoru databáze viz "Konfigurace modulu protokolování MFT" na stránce 695.

Zachování průběhu a protokolování zpráv pomocí modulu plug-in produktu IBM MQ Explorer

Je-li poprvé spuštěna instance modulu plug-in produktu IBM MQ Explorer , vytvoří instance trvalý odběr v koordinačním správci front. Tento trvalý odběr se používá ke shromažďování informací, které se zobrazují v zobrazeních **Protokol přenosu** a **Průběh aktuálního přenosu** .

Název trvalého odběru má předponu, která ukazuje, že odběr byl vytvořen modulem plug-in produktu 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 aktivním způsobem používán instancí modulu plug-in IBM MQ Explorer .

Použití trvalého odběru v koordinačním správci front může způsobit vytvoření zpráv v systému SYSTEM.MANAGED.DURABLE fronty. Máte-li síť s vysokou hlasitost Managed File Transfer , použijte modul plug-in produktu IBM MQ Explorer zřídka nebo obě tato data, tato zpráva může vyplnit lokální souborový systém.

Pokud toto chování nechcete, můžete určit, že modul plug-in IBM MQ Explorer bude používat netrvalý odběr vůči koordinačnímu správci front. 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 publikací ve frontě IBM MQ

Chcete-li uložit protokol nebo zprávy o průběhu ve frontě produktu IBM MQ , nakonfigurujte odběr v koordinačním správci front, který předává zprávy do této fronty. Chcete-li například předat 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)
```

Po předání zpráv protokolu do fronty produktu IBM MQ jsou tyto zprávy uloženy ve frontě, dokud nejsou zpracovány aplikací produktu IBM MQ , která danou frontu používá.

Zápis aplikací, které spravují trvalý odběr, do systému SYSTEM.FTE

Aplikace, které spravují své vlastní trvalé odběry, můžete napsat do SYSTEM.FTE se používá k použití jednoho z rozhraní API podporovaných produktem IBM MQ. Tyto aplikace mohou přijímat zprávy fronty nebo protokolu produktu IBM MQ a správně je podle vašich obchodních potřeb provádět.

Další informace o dostupných rozhraních programování aplikací naleznete v tématu Vývoj aplikací.

Konfigurace modulu protokolování MFT

Když produkt Managed File Transfer přenáší soubory, publikuje informace o svých akcích na téma v koordinačním správci front. Modul pro protokolování databáze je volitelná komponenta produktu Managed File Transfer , kterou lze použít ke kopírování těchto informací do databáze pro účely analýzy a auditu.

Existují tři verze modulu protokolování:

- ULW samostatný modul protokolování souborů
- samostatný modul protokolování databáze
- Modul protokolování produktu Java Platform, Enterprise Edition (Java EE)

Zapisovače protokolu na serveru IBM i

IBM i

Moduly protokolování produktu Managed File Transfer nejsou na platformě IBM i podporovány.

Samostatný modul protokolování souborů

ULW

Samostatný modul protokolování souborů je proces produktu Java , který je spuštěn v systému, který je hostitelem koordinačního správce front, nebo v systému, který je hostitelem správce front s možností připojení ke koordinačnímu správci front. Modul protokolování samostatných souborů používá vazby produktu IBM MQ k připojení k přidruženému správci front. Samostatný modul protokolování je vytvořen pomocí příkazu **fteCreateLogger** .

Windows Samostatný zapisovač protokolu souborů můžete spustit jako službu Windows , abyste se ujistili, že modul protokolování souborů bude pokračovat při odhlášení z relace Windows a lze jej nakonfigurovat tak, aby se spouštěl automaticky při restartu systému. Další informace viz téma “Instalace samostatného modulu protokolování souborů produktu MFT” na stránce 696.

Modul protokolování samostatných souborů není podporován na následujících platformách:

- z/OS z/OS
- IBM i IBM i

Samostatný modul protokolování databáze

Samostatný modul protokolování databáze je aplikace produktu Java , kterou instalujete na systém, který je hostitelem správce front a databáze. Samostatný modul protokolování databáze je často nainstalován ve stejném systému jako koordinační správce front, avšak může být také nainstalován na stejném systému jako správce front s možností připojení ke koordinačnímu správci front. Samostatný modul protokolování databáze používá vazby produktu IBM MQ pro připojení k přidruženému správci front a ovladač typu 2 nebo 4 ovladače JDBC pro připojení k databázi Db2 nebo k databázi Oracle . Tyto typy připojení jsou povinné, protože samostatný modul pro protokolování databází používá podporu XA správce front pro koordinaci globální transakce nad správcem front i databází a tím chrání data.

Windows Používáte-li systém Windows , můžete samostatné moduly protokolování spouštět jako služby produktu Windows , abyste zajistili, že moduly protokolování budou pokračovat v činnosti při odhlášení z relace produktu Windows . Další informace viz “Instalace samostatného modulu protokolování databáze produktu MFT” na stránce 703 pro samostatný modul protokolování databáze.

Modul protokolování databáze Java EE

Modul pro protokolování databáze produktu Java EE je k dispozici jako soubor EAR, který instalujete na aplikační server. To může být výhodnější než použití samostatného modulu protokolování databáze v případě, že máte k dispozici existující prostředí aplikačního serveru Java EE , protože modul protokolování databáze produktu Java EE může být spravován spolu s ostatními podnikovými aplikacemi. Můžete také nainstalovat modul protokolování databáze produktu Java EE na samostatném systému do systémů, které jsou hostiteli serveru IBM MQ a databáze. Modul protokolování databáze Java EE je podporován pro použití s databázemi Db2 a Oracle . Modul protokolování databáze produktu Java EE rovněž podporuje produkt Oracle Real Application Clusters, je-li instalován v systému WebSphere Application Server 7.0.

Pokyny, jak nakonfigurovat modul protokolování, naleznete v následujících tématech:

- “Instalace samostatného modulu protokolování souborů produktu MFT” na stránce 696
- “Instalace samostatného modulu protokolování databáze produktu MFT” na stránce 703
- “Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT” na stránce 708

ULW Instalace samostatného modulu protokolování souborů produktu MFT

Samostatný modul protokolování souborů je proces produktu Java , který se musí připojit ke koordinačnímu správci front pomocí vazeb IBM MQ . Chcete-li definovat samostatný modul protokolování souborů, použijte příkaz **fteCreateLogger** a postupujte podle kroků uvedených v tomto tématu.

Informace o této úloze

Další informace o samostatném registrátoru souborů viz “Konfigurace modulu protokolování MFT” na stránce 695. Kroky v tomto tématu konfigurují modul protokolování pro připojení ke koordinačnímu správci front. Alternativní konfigurace modulu protokolování viz “Alternativní konfigurace pro samostatný modul protokolování produktu MFT” na stránce 707 .

Modul protokolování samostatných souborů není podporován na následujících platformách:

- z/OS z/OS
- IBM i IBM i

Postup

1. Ujistěte se, že máte nainstalovanou komponentu produktu Managed File Transfer Logger . Další informace naleznete v tématu Volby produktu Managed File Transfer .
2. Spuštěním příkazu **fteCreateLogger** specifikující koordinačního správce front a nastavením parametru -loggerType na hodnotu FILE vytvořte modul protokolování samostatného souboru. Další informace viz fteCreateLogger.
3. Volitelné: Chcete-li použít vlastní formát, pak můžete upravit soubor XML vytvořený příkazem **fteCreateLogger** . Definice formátu protokolu se nachází v souboru `FileLoggerFormat.xml` . Další informace viz téma “Formát samostatného modulu protokolování souborů produktu MFT” na stránce 697.
4. Spuštěním příkazů MQSC poskytnutých příkazem **fteCreateLogger** pro koordinačního správce front vytvořte fronty modulu protokolování.
5. Identifikujte uživatele, aby spustil proces modulu protokolování, a nakonfigurujte oprávnění pro tohoto uživatele. Další informace viz téma “Konfigurace uživatelského přístupu pro samostatný modul protokolování souborů produktu MFT” na stránce 703.
6. Volitelné: Samostatný modul protokolování souborů můžete nakonfigurovat dále tak, že upravíte soubor `logger.properties` vytvořený při spuštění příkazu **fteCreateLogger** . Tento soubor je soubor 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 vlivu naleznete v tématu Vlastnosti konfigurace modulu protokolování produktuMFT.
7. Windows
   Volitelné: Používáte-li systém Windows , můžete modul protokolování samostatných souborů spustit jako službu Windows . Spusťte příkaz **fteModifyLogger** s argumentem **-s** . Další informace viz fteModifyLogger.
8. Spusťte modul protokolování samostatného souboru pomocí příkazu **fteStartLogger** . Další informace viz fteStartLogger.

   Pokud jste provedli předchozí krok a použili příkaz **fteModifyLogger** s parametrem **-s** v systému Windows, modul protokolování samostatných souborů se spouští jako služba Windows .
9. Zkontrolujte výstup modulu protokolování. Modul protokolování samostatného souboru generuje dva typy výstupu, data auditu přenosu souborů a diagnostická data zapisovače protokolu. Data auditu přenosu souborů lze nalézt v *MQ_DATA_PATH*`/mqft/logs/`*coordination_qmgr_name*`/loggers/`*logger_name*`/logs`. Diagnostická data modulu protokolování lze nalézt v *MQ_DATA_PATH*`/mqft/logs/`*coordination_qmgr_name*`/loggers/`*logger_name*
10. Modul protokolování můžete zastavit pomocí příkazu **fteStopLogger** . Další informace viz fteStopLogger.

Výsledky

ULW *Formát samostatného modulu protokolování souborů produktu MFT*

Formát informací o zprávě zapisovaných modulem protokolování souborů může být definován 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 Výchozí formát protokolu výchozího protokolu modulu protokolování produktuMFT.

Chcete-li určit vlastní formát protokolu, upravte soubor `FileLoggerFormat.xml` .

Vlastní definice formátu protokolu

Definice formátu protokolu se skládá ze sady typů zpráv s každým typem zprávy, který 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 se obsah umístí do řádků generovaných pro výstup do souborů protokolu. Toto je například definice 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, jako je tento:

```
2011-11-25T10:53:04;414d5120514d5f67627468696e6b20206466cf4e20004f02;[CSTR];
  AGENT1;AGENT_QM;Managed Call;executable;echo;call test;
```

Vložky zadané 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 části Standard-lone file logger format XSD(Standardní formát souboru XSD).

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 formátů 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 v souboru protokolu pro každou zprávu protokolu spotřebovanou z dílčího tématu SYSTEM.FTE/Log . To vede k jednoduchému případu,

kdy se adresy XPATH zadané v definici formátu protokolu vztahují ke kořenu zprávy. Toto jsou typy zpráv, které používají tuto metodu k zápisu výstupu:

```
callCompleted
callStarted
monitorAction
monitorCreate
monitorFired
notAuthorized
scheduleDelete
scheduleExpire
scheduleSkipped
scheduleSubmitInfo
scheduleSubmitTransfer
transferStarted
transferCancelled
transferComplete
transferDelete
```

Druhá metoda použitá k zápisu zprávy protokolu používá více řádků ke znázornění 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 jednotlivé položky v rámci sady přenosů, je pro použití této položky jako její kořen XPATH vyžadována zadaná položka XPATH. Toto jsou typy zpráv, které používají tuto metodu k zápisu výstupu:

```
scheduleSubmitTransferSet
transferProgress
```

Pro každou položku v sadě přenosu je zapsán řádek výstupu. Informace, které chcete opravit pro všechny položky v sadě přenosu, mohou stále používat adresy XPATH vztahující se ke kořeni zprávy protokolu. V následujícím zjednodušeném příkladu definice formátu `transferProgress` je to časové razítko a ID přenosu, které jsou pevné. Všechny informace, které se vztahují k položce jako její kořen, se budou u jednotlivých zapsaných řádků lišit. V tomto příkladě 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 o jednom nebo více řádcích 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 své rozvržení přizpůsobené pomocí atributů **`width`** a **`ignoreNull`** prvku vložení. Příklad:

```
<insert type="user" width="48" ignoreNull="false">/transaction/@ID</insert>
```

V tomto příkladě vezme vložení informace nalezené ve zprávě protokolu na `/transaction/@ID` a ořízne ji na 48 znaků před tím, než se zapíše do protokolu. Pokud má obsah souboru `/transaction/@ID` hodnotu null, zapíše řetězec null po doplnění do 48 znaků, protože atribut `ignoreNull` je nastaven na hodnotu `false`. Je-li parametr `ignoreNull` nastaven na hodnotu `true` , bude místo toho zapsán prázdný řetězec, doplněný na 48 znaků. Nastavení width="0 " znamená, že šířka sloupce není oříznuta, neznamená to, že by šířka byla oříznuta na 0. Atribut `ignoreNull` lze použít tímto způsobem ke zjištění v protokolu, když je nalezena hodnota null, když nebyla očekávána. To může být užitečné při ladění nové definice souboru protokolu.

Vložky definované uživatelem

Vložka uživatele obsahuje adresu XPATH pro informace, které mají být zapsány v této operaci vložení. Tato adresa odkazuje na část informací, která se nachází ve zprávě protokolu FTE. Další informace o formátech zpráv protokolu viz:

- Formáty zpráv protokolu přenosu souborů
- Formáty zpráv protokolu přenosu naplánovaných souborů
- Formát zprávy protokolu monitoru MFT

Systémem definovaná vložení

Systémem definovaná vložení obsahují klíčové slovo, které odkazuje na část informací, které buď nelze nalézt ve zprávě protokolu, nebo není jednoduché definovat pomocí jazyka XPATH.

Podporovány jsou následující systémy:

- `type` -Zapíše typ zprávy protokolu v krátkém formátu.
- `callArguments` -zapisuje sadu argumentů dodaných do spravovaného volání ve formátu odděleném mezerou.
- `transferMetaData` -Zapíše sadu položek metadat definovaných pro přenos ve formátu *key=value* oddělených čárkami.

Následující tabulka obsahuje hodnotu typu "type" pro systémové hodnoty vložení pro každý typ zprávy.

Tabulka 51. Souhrn podporovaných typů zpráv a jejich systémových vložení typu "type".

Typ zprávy	**Hodnota vložení systému "type"**
callCompleted	[CCOM]
callStarted	[CSTR]
monitorAction	[MACT]
monitorCreate	[MRCT]
monitorFired	[JEDLE]
notAuthorized	[AUTH]

Tabulka 51. Souhrn podporovaných typů zpráv a jejich systémových vložení typu "type". (pokračování)	
Typ zprávy	**Hodnota vložení systému "type"**
scheduleDelete	[SDEL]
scheduleExpire	[SEXP]
scheduleSkipped	[SSKP]
Informace o scheduleSubmit	[SSIN]
Přenos scheduleSubmit	[SSTR]
scheduleSubmitTransferSet	[SSS]
transferStarted	[TSTR]
transferCancelled	[TCAN]
transferComplete	[TCOM]
transferDelete	[TDEL]
transferProgress	[TPRO]

ULW *Vyloučení typů zpráv ze samostatného modulu protokolování souborů produktu MFT*
Chcete-li vyloučit určitý typ zprávy z výstupu modulu protokolování souborů, můžete použít prázdné prvky typu zprávy.

Příklad

Například následující definice formátu zastaví `transferProgress` zprávy jsou výstupem 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>
```

ULW *Definování vlastních formátů pro samostatný modul protokolování souborů produktu MFT*
Je možné definovat podmnožinu vlastních typů zpráv v rámci definice formátu protokolu ke snížení množství konfigurace požadované k úpravě formátu souboru protokolu.

Informace o této úloze

Není-li prvek `messageTypes` zahrnut do souboru `FileLoggerFormat.xml` , formát pro tento typ zprávy používá výchozí formát. Musíte pouze uvést formáty, které chcete, aby se lišily od předvolby.

Příklad

V tomto příkladu definice formátu nahrazuje výchozí formát pro typ zprávy `transferStarted` s touto zmenšenou verzí, která obsahuje pouze uživatele, který přenos spustil. 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 modulu protokolování samostatného souboru produktu MFT

Formát XSD formátu samostatného souboru XSD

ULW *Omezení duplicitních zpráv v samostatném registrátoru souborů MFT*

V protokolu samostatného zapisovače protokolu souborů se mohou objevit duplicitní zprávy protokolu. Pomocí souboru `logger.properties` můžete vyladit samostatný modul protokolování souborů a snížit počet duplikátů.

Duplicitní zprávy v protokolu modulu protokolování souborů

Dojde-li k selhání, může být zapsána zpráva protokolu do protokolu samostatného modulu protokolování souborů bez spotřeby zprávy protokolu ze systému SYSTEM.FTE/Log# téma potvrzované produktem IBM MQ. Pokud k tomu dojde, když se samostatný modul protokolování souborů restartuje, načte stejnou zprávu podruhé a znovu ji zapíše do souboru protokolu. Naplánujte možnost těchto duplikátů při pohledu na soubory protokolu buď ručně, nebo při jejich automatickém zpracování. Jako pomoc při zjišťování duplikátů umístí samostatný modul protokolování souborů následující zprávu do souboru protokolu při jeho spuštění:

```
BFGDB0054I: The file logger has successfully started
```

Duplikáty se stávají vždy kolem času zahájení modulu pro protokolování samostatných souborů, protože se jedná o poslední zprávu, která byla přečtena před zpracováním předchozí instance. Vědět, kdy byla nová instance spuštěna, můžete zjistit, zda se mají očekávat duplikáty, a zda je třeba je zpracovat, či nikoli.

Snížení počtu duplikátů

Samostatné skupiny registrátorů souborů dohromady protokolují zprávy, které zpracovává, do transakcí za účelem zlepšení výkonu. Tato velikost dávky je maximální počet duplicitních zpráv, které se mohou zobrazit v případě selhání. Chcete-li snížit počet duplikátů, můžete vyladit následující vlastnost v souboru `logger.properties` :

```
wmqfte.max.transaction.messages
```

Například nastavením tohoto na 1 se maximální počet duplicitních zpráv sníží na 1. Uvědomte si, že změna této hodnoty má vliv na výkon vašeho samostatného modulu protokolování souborů, takže se vyžaduje důkladné testování, abyste se ujistili, že to nemá nepříznivý vliv na váš systém.

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 Vlastnosti konfigurace modulu protokolování produktuMFT

ULW ***Konfigurace uživatelského přístupu pro samostatný modul protokolování souborů produktu MFT***

V testovacím prostředí můžete přidat veškerá nová oprávnění potřebná pro běžný uživatelský účet. V produkčním prostředí se doporučuje vytvořit nového uživatele s minimálními oprávněními nutnými k provedení úlohy.

Informace o této úloze

Samostatný modul protokolování souborů a produkt IBM MQ je třeba nainstalovat na jeden systém. Nakonfigurujte oprávnění uživatele následujícím způsobem:

Postup

1. Ujistěte se, že uživatel má oprávnění ke čtení a tam, kde je to nutné, soubory instalované jako součást 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 je-li to nezbytné pro diagnostické trasovací soubory a soubory FFDC (First Failure Data Capture).
3. Ujistěte se, že uživatel má svou vlastní skupinu, a že také není ve skupinách s povoleními v rámci koordinačního správce front v režimu wi-dese. Uživatel by neměl být ve skupině mqm. Na určitých platformách má skupina personálu automaticky také udělen přístup správce front; uživatel modulu pro protokolování samostatných souborů by neměl být ve skupině personálu. Záznamy oprávnění můžete zobrazit pro správce front jako takový a pro objekty v něm obsažené pomocí produktu IBM MQ Explorer. Klepněte pravým tlačítkem myši na objekt a vyberte volbu **Oprávnění k objektu > Správa záznamů oprávnění**. Na příkazovém řádku můžete použít příkazy dspmqaut (display authority) nebo dmpmqauth (dump authority).
4. Použijte okno **Spravovat záznamy oprávnění** v produktu IBM MQ Explorer nebo příkaz setmqaut (grant nebo revoke authority) , abyste přidali oprávnění pro vlastní skupinu uživatele (v systému UNIXjsou oprávnění k produktu IBM MQ přidružena pouze ke skupinám, nikoli k jednotlivým uživatelům). Požadované orgány jsou následující:
   - Připojte se ke správci front (knihovny produktu IBM MQ Java vyžadují oprávnění pro zjišťování oprávnění k práci).
   - Přihlaste se k odběru oprávnění na SYSTEM.FTE .
   - Oprávnění k umístění zadejte na SYSTEM.FTE.LOG.RJCT.*název_modulu_protokolování* .
   - Získejte oprávnění k SYSTEM.FTE.LOG.CMD. Fronta*logger_name* .

   Jako výchozí názvy jsou použity výchozí názvy fronty odmítnutí a příkazu. Pokud jste při konfiguraci samostatných front modulu protokolování samostatných souborů vybrali různé názvy front, přidejte místo nich oprávnění k těmto názvům front.

Instalace samostatného modulu protokolování databáze produktu MFT

Chcete-li instalovat a konfigurovat samostatný modul pro protokolování databáze, postupujte podle těchto kroků.

Informace o této úloze

Důležité: Moduly protokolování produktu Managed File Transfer nejsou na platformě IBM i podporovány.

Další informace o samostatném modulu protokolování databáze naleznete v tématu “Konfigurace modulu protokolování MFT” na stránce 695.

Poznámka: Nemůžete spustit více než jeden modul protokolování databáze (samostatný nebo Java EE) oproti stejnému schématu v databázi v jednom okamžiku. Pokus o provedení této operace by vedl ke kolizím při pokusu o zápis dat protokolu přenosu do databáze.

Postup

1. Nainstalujte svůj databázový software pomocí dokumentace pro vaši databázi.

   Je-li podpora JDBC pro vaši databázi volitelnou komponentou, musíte nainstalovat tuto komponentu.
2. Spusťte příkaz **fteCreateLogger** , který nastaví parametr **-loggerType** na DATABASE a vytvoří se samostatný modul protokolování databáze. Další informace viz fteCreateLogger.

   Výchozí název schématu je FTELOG. Pokud používáte jiný název schématu než FTELOG, musíte upravit poskytnutý soubor SQL odpovídající vaší databázi, `ftelog_tables_db2.sql` nebo `ftelog_tables_oracle.sql`, aby se tento název schématu odrazil, a teprve pak pokračujte dalším krokem. Další informace viz wmqfte.database.schema v vlastnostech konfigurace modulu protokolování produktuMFT.
3. Vytvořte požadované databázové tabulky pomocí nástrojů databáze.

   Multi V systému Multiplatformsobsahují soubory `ftelog_tables_db2.sql` a `ftelog_tables_oracle.sql` příkazy SQL, které lze spustit pro vytvoření tabulek.

   z/OS V systému z/OSzávisí soubor, který je třeba spustit, na verzi produktu Db2 for z/OS , kterou používáte:

   - Pro Db2 for z/OS 9.0 a starší spusťte soubor `ftelog_tables_zos.sql` , abyste vytvořili tabulky. Tento soubor vytváří tabulky s použitím datového typu INTEGER pro pole, která označují velikost přenesených souborů a ID tabulky přidružené k jednotlivým přenosům.
   - Pro produkt Db2 for z/OS 9.1 a novější spusťte soubor `ftelog_tables_zos_bigint.sql` pro vytvoření tabulek. Tento soubor vytváří tabulky s datovým typem BIGINT pro pole, která označují velikost přenesených souborů a ID tabulky přidružené k jednotlivým přenosům.
4. Chcete-li vytvořit fronty modulu protokolování, spusťte příkazy MQSC poskytnuté příkazem **fteCreateLogger** pro správce front příkazů modulu protokolování. Modul pro protokolování samostatné databáze používá dvě fronty v koordinačním správci front. První fronta je fronta příkazů, do které jsou umisťována zprávy pro řízení operace samostatného modulu protokolování databáze. Výchozí název této fronty příkazů je SYSTEM.FTE.LOG.CMD.*název_modulu_protokolování*. Druhá fronta je fronta odmítnutí. Protože samostatný modul protokolování databáze nikdy nevyřadí zprávy protokolu, pokud modul protokolování narazí na zprávu, kterou nedokáže zpracovat, umístí zprávu do fronty odmítnutí k prozkoumání a možné přepracování. K tomuto účelu se nedoporučuje používat frontu nedoručených zpráv správce front, protože odmítnuté zprávy nemají záhlaví DLH a protože odmítnuté zprávy by neměly být zkombinovány se zprávami vkládané do fronty nedoručených zpráv z jiných důvodů. Výchozí název pro frontu odmítnutí je SYSTEM.FTE.LOG.RJCT.*název_modulu_protokolování*. Tyto dvě fronty jsou definovány ve skriptových souborech MQSC generovaných příkazem **fteCreateLogger** .
5. Zvolte uživatele a nakonfigurujte oprávnění.
6. Volitelné: Samostatný zapisovač protokolu databáze můžete dále konfigurovat tak, že upravíte soubor `logger.properties` vytvořený příkazem **fteCreateLogger** v kroku “2” na stránce 704. Tento soubor je soubor 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 viz téma Vlastnosti konfigurace modulu protokolování produktuMFT.
7. Windows

   Volitelné: Používáte-li systém Windows , můžete modul protokolování samostatné databáze spustit jako službu Windows . Spusťte příkaz **fteModifyLogger** s argumentem **-s** . Další informace viz fteModifyLogger.

8. Volitelné: Je-li používaná databáze Oracle nebo pokud se připojujete k databázi Db2 vzdáleně, budete muset zadat jméno uživatele a heslo, které bude modul protokolování používat pro ověření s databázovým serverem. Toto jméno uživatele a heslo je uvedeno v souboru pověření, který je v souladu s formátem definovaným schématem produktu `MQMFTCredentials.xsd` . Další informace viz Formát souboru pověření MFT. Po vytvoření souboru pověření je třeba určit umístění souboru pověření v souboru `logger.properties` pomocí vlastnosti `wmqfte.database.credentials.file` .
9. Spusťte samostatný modul protokolování databáze pomocí příkazu **`fteStartLogger`** . Standardně se samostatný modul protokolování databáze spouští na pozadí a samostatný modul protokolování databáze umisťuje výstup do souboru v adresáři `logs` . Chcete-li spustit modul protokolování samostatné databáze v popředí a vytvořit výstup na konzolu i do souboru protokolu, přidejte do příkazu **`fteStartLogger`** parametr **`-F`** .

   Pokud jste provedli předchozí krok a použili příkaz **`fteModifyLogger`** s parametrem **`-s`** v systému Windows, je samostatný modul protokolování databáze spuštěn jako služba Windows .

Použití produktu MFT se vzdálenou databází

Modul protokolování produktu Managed File Transfer můžete použít ke komunikaci s databází ve vzdáleném systému.

Informace o této úloze

Pokud máte nainstalovanou databázi na jiném počítači než počítač Managed File Transfer , proveďte následující kroky. Pokud není uvedeno jinak, kroky platí pro produkty Db2 i Oracle .

Postup

1. Nainstalujte databázového klienta na systém, na který jste nainstalovali produkt Managed File Transfer .
2. Přidejte vzdálený databázový server do vaší konfigurace klienta lokální databáze. Tato aktualizace konfigurace je nutná k tomu, aby produkty Managed File Transfer a IBM MQ správně přistupovaly k databázi.
3. Určete nové vlastnosti v souboru `logger.properties` pro připojení k databázi pomocí souboru pověření: **`wmfte.database.credentials.file`**.

   Poznámka: Starší 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 zamítnuté. Místo toho použijte **`wmfte.database.credentials.file`** .
4. **PouzeOracle :** Chcete-li povolit vzdálené připojení k databázi, změňte objekt stanza 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`je tato změna zvýrazněna tučným písmem.
5. **PouzeOracle :** Určete hostitele a port v souboru `logger.properties` s použitím vlastností **`wmqfte.oracle.host`** a **`wmqfte.oracle.port`** . Výchozí hodnoty pro hostitele a port umožňují pracovat s lokálním databázovým klientem, takže pokud jste již dříve pracovali s lokální databází, možná jste tyto hodnoty nenastavili.

Související odkazy

Vlastnosti konfigurace modulu protokolování produktu MFT

Konfigurace uživatelského přístupu pro samostatný modul protokolování databáze produktu MFT

V testovacím prostředí můžete přidat veškerá nová oprávnění potřebná pro běžný uživatelský účet. V produkčním prostředí se doporučuje vytvořit nového uživatele s minimálními oprávněními nutnými k provedení úlohy.

Informace o této úloze

Počet a typ uživatelských účtů, které potřebujete ke spuštění samostatného modulu protokolování databáze, závisí na počtu systémů, které používáte. Můžete nainstalovat samostatný modul protokolování databáze, IBM MQ a vaši databázi na jednom systému nebo na dvou systémech. Samostatný modul protokolování databáze musí být na stejném systému jako produkt IBM MQ. Tyto komponenty mohou být instalovány v následujících topologiích:

Samostatná databáze Logger, IBM MQ a databáze na stejném systému
Můžete definovat jediného uživatele operačního systému pro použití se všemi třemi komponentami. Jedná se o vhodnou konfiguraci pro samostatný modul protokolování databáze. Modul protokolování samostatné databáze používá režim vazeb pro připojení k databázi IBM MQ a nativní připojení pro připojení k databázi.

Samostatný modul protokolování databáze a produkt IBM MQ na jednom systému, databáze na samostatném systému
Vytvoříte dva uživatele pro tuto konfiguraci: uživatel operačního systému na systému, na kterém běží samostatný modul protokolování databáze, a uživatel operačního systému se vzdáleným přístupem k databázi na databázovém serveru. Jedná se o vhodnou konfiguraci pro samostatný modul protokolování databáze pomocí vzdálené databáze. Modul protokolování samostatné databáze používá režim vazeb pro připojení k databázi IBM MQ a připojení klienta pro přístup k databázi.

Jako příklad předpokládejme, že zbytek těchto pokynů předpokládá, že se uživatel nazývá `ftelog`, ale můžete použít libovolné jméno uživatele. Nakonfigurujte oprávnění uživatele následujícím způsobem:

Postup

1. Ujistěte se, že uživatel má oprávnění ke čtení a tam, kde je to nutné, soubory instalované jako součást instalace produktu Managed File Transfer Remote Tools a Documentation .
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 je-li to nezbytné pro diagnostické trasovací soubory a soubory FFDC.
3. Ujistěte se, že uživatel má svou vlastní skupinu, a také není ve všech skupinách s povoleními na koordinačním správci front v režimu wide-sarand. Uživatel by neměl být ve skupině mqm. Na určitých platformách má skupina personálu automaticky také udělen přístup správce front; samostatný uživatel modulu pro protokolování databáze by neměl být ve skupině zaměstnanců. Můžete zobrazit záznamy oprávnění pro samotný správce front a pro objekty v něm obsažené v produktu IBM MQ Explorer. Klepněte pravým tlačítkem myši na objekt a vyberte volbu **Oprávnění k objektu > Správa záznamů oprávnění**. Na příkazovém řádku můžete použít příkazy dspmqaut (display authority) nebo dmpmqauth (dump authority).
4. Použijte okno **Spravovat záznamy oprávnění** v produktu IBM MQ Explorer nebo příkaz setmqaut (grant nebo revoke authority) , abyste přidali oprávnění pro vlastní skupinu uživatele (v systému UNIXjsou oprávnění k produktu IBM MQ přidružena pouze ke skupinám, nikoli k jednotlivým uživatelům). Požadované orgány jsou následující:
   - Připojte se ke správci front (knihovny produktu IBM MQ Java vyžadují oprávnění pro zjišťování oprávnění k práci).
   - Přihlaste se k odběru oprávnění na SYSTEM.FTE .
   - Oprávnění k umístění zadejte na SYSTEM.FTE.LOG.RJCT.*název_modulu_protokolování* .
   - Získejte oprávnění k SYSTEM.FTE.LOG.CMD. Fronta*logger_name* .

   Jako výchozí názvy jsou použity výchozí názvy fronty odmítnutí a příkazu. Pokud jste při konfiguraci samostatných front modulu pro protokolování databáze vybrali různé názvy front, přidejte místo nich oprávnění k těmto názvům front.
5. Proveďte konfiguraci uživatele, která je specifická pro databázi, kterou používáte.
   - Pokud je vaše databáze Db2, proveďte následující kroky:

     Pro správu uživatelů databází pomocí produktu Db2existuje několik mechanizmů. Tyto pokyny se vztahují na výchozí schéma založené na uživatelích operačního systému.

  - Ujistěte se, že uživatel produktu `ftelog` není ve všech administračních skupinách produktu Db2 (například db2iadm1, db2fadm1nebo dasadm1).
  - Udělte uživateli oprávnění k připojení k databázi a oprávnění k výběru, vložení a aktualizaci tabulek, které jste vytvořili jako součást kroku 2: vytvoření požadovaných databázových tabulek .
- Je-li vaše databáze Oracle, proveďte následující kroky:
  - Ujistěte se, že uživatel produktu `ftelog` není ve všech administračních skupinách Oracle (například ora_dba on Windows nebo dba na UNIX)
  - Udělte uživateli oprávnění k připojení k databázi a oprávnění k výběru, vložení a aktualizaci tabulek, které jste vytvořili jako součást kroku 2: vytvoření požadovaných databázových tabulek .

Alternativní konfigurace pro samostatný modul protokolování produktu MFT

Samostatný modul protokolování produktu Managed File Transfer bez ohledu na to, zda se jedná o soubor nebo typ databáze, je ve stejném systému jako koordinační správce front a je připojen ke koordinačnímu správci front v režimu vazeb IBM MQ . Lze jej však také instalovat ve stejném systému jako správce front, který má propojitelnost se koordinačním správcem front. Samostatný modul protokolování přijímá zprávy pomocí odběru, který je samostatný modul protokolování automaticky vytvořen. Jedná se o konfiguraci popsanou v pokynech k instalaci.

Pokud však máte k dispozici specifické aspekty zabezpečení, můžete nakonfigurovat samostatný modul protokolování tak, aby přijímal zprávy dvěma dalšími způsoby řízenými vlastností wmqfte.message.source.type . Tato vlastnost je popsána v části Vlastnosti konfigurace modulu protokolování produktuMFT.

Administrativní odběr

Samostatný modul protokolování standardně vytvoří svůj vlastní odběr do systému SYSTEM.FTE/Log/# tématu s použitím výchozích voleb trvalých odběrů a spravovaného odběru (to znamená, že správce front řídí záložní frontu používanou k uchování zpráv před jejich předáním do aplikace). Jsou-li v odběru nebo ve frontě vyžadovány další volby, můžete místo toho vytvořit vlastní odběr, nastavit vyžadované volby a nakonfigurovat samostatný modul protokolování tak, aby místo něj používal tento odběr. Nezapomeňte přidat oprávnění pro samostatný modul protokolování pro použití odběru, který jste vytvořili.

Příklad použití této konfigurace je rozdělení prostoru protokolu pomocí dvou odběrů se zástupnými znaky, k odeslání protokolů 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, každý se svým vlastním souborem `logger.properties` odkazujícím na požadovaný odběr a jeho vlastní frontu příkazů a frontu odmítnutí.

Chcete-li shromažďovat zprávy protokolu pouze z agentů, jejichž názvy začínají na ACCOUNTING, vytvořte objekt odběru ve svém koordinačním správci front s řetězcem tématu SYSTEM.FTE/Log/ ACCOUNTING*. Nastavte hodnotu **Použití zástupného znaku** na hodnotu **Zástupný znak na úrovni znaku**. Musíte také přidat položky do souboru `logger.properties` pro váš modul protokolování. Vytváříte-li například 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 uvést více omezující řetězec tématu, ale nemůžete uvést méně omezující řetězec. Pokud uvedete méně restriktivní řetězec v chybě, všechny publikace, které se vztahují k řetězci tématu jiným než SYSTEM.FTE/Log/ přejde do fronty odmítnutí a samostatný modul protokolování vygeneruje chybovou zprávu BFGDB0002E. Tato chybová zpráva znamená, že došlo k problému se samostatnou konfigurací modulu protokolování.

Fronta

Typickou topologií je místo, kde se samostatný modul protokolování spouští ve stejném systému jako koordinačního správce front. Pokud to není možné, můžete vytvořit odběr u koordinačního správce front s použitím fronty v jiném správci front jako místo určení odběru (buď pomocí definice vzdálené fronty, nebo pomocí vlastnosti DESTQMGR odběru). Modul protokolování lze poté spustit na 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. Musíte definovat frontu odmítnutí a frontu příkazů na stejném správci front, ke kterému se připojuje samostatný modul protokolování. Správci front musí být v produktu IBM WebSphere MQ 7.5 nebo pozdější.

Chcete-li například shromáždit zprávy protokolu, které jsou umístěny do fronty USER.QUEUE podle odběru přidejte tyto položky do souboru `logger.properties` :

```
wmqfte.message.source.type=queue
wmqfte.message.source.name=USER.QUEUE
```

Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT

Chcete-li instalovat a konfigurovat modul protokolování databáze JEE pro použití s produktem Managed File Transfer, postupujte podle těchto pokynů.

Informace o této úloze

Další informace o registrátoru databáze Java EE naleznete v tématu “Konfigurace modulu protokolování MFT” na stránce 695.

Poznámka: Modul pro protokolování databáze produktu Java EE nelze spustit zároveň se samostatným zapisovačem protokolu, pokud tyto moduly protokolování nepoužívají oddělené instance databáze.

Postup

1. Před instalací modulu pro protokolování databáze produktu Java EE je třeba připravit prostředí. Postupujte podle pokynů uvedených v tématu “Příprava na instalaci modulu protokolování databáze Java EE pro produkt MFT” na stránce 709.
2. Modul protokolování databáze produktu Java EE instalujete do aplikačního serveru vyhovujícího produktu Java Platform, Enterprise Edition (Java EE). Pokyny naleznete v těchto tématech:
   - “Instalace modulu protokolování databáze Java EE pro produkt MFT s produktem WebSphere Application Server 7.0” na stránce 712
   - “Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT s produktem WebSphere Application Server Community Edition” na stránce 716

Související úlohy

“Příprava na instalaci modulu protokolování databáze Java EE pro produkt MFT” na stránce 709
Před instalací modulu pro protokolování databáze produktu Java EE postupujte podle těchto pokynů a připravte prostředí produktu Managed File Transfer .

“Instalace modulu protokolování databáze Java EE pro produkt MFT s produktem WebSphere Application Server 7.0” na stránce 712
Postupujte podle těchto pokynů, chcete-li instalovat a konfigurovat modul protokolování databáze produktu Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s produktem WebSphere Application Server 7.0.

“Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT s produktem WebSphere Application Server Community Edition” na stránce 716
Postupujte podle těchto pokynů, chcete-li instalovat a konfigurovat modul protokolování databáze produktu Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s produktem WebSphere Application Server Community Edition.

“Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro produkt MFT” na stránce 720
Když konfigurujete modul protokolování databáze Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer, potřebujete uživatelské účty pro přístup k databázi IBM MQ, k databázi a k operačnímu systému. Počet uživatelů operačního systému, které se požadují, závisí na počtu systémů, které používáte k hostování těchto komponent.

“Migrace ze samostatného modulu protokolování databáze do modulu protokolování databáze Java EE pro produkt MFT” na stránce 722
Můžete migrovat ze samostatného modulu protokolování databáze na modul protokolování databáze produktu Java EE . Je třeba zastavit samostatný modul protokolování databáze a nainstalovat modul protokolování databáze JEE. Chcete-li se vyhnout ztrátě nebo duplikaci záznamů protokolu, musíte zastavit publikování zpráv do SYSTEM.FTE před zastavením samostatného modulu pro protokolování databáze a po instalaci modulu pro protokolování databáze produktu Java EE jej restartujte. Před migrací zálohujte svou databázi.

Související odkazy

Oprávnění pro modul protokolování MFT

Příprava na instalaci modulu protokolování databáze Java EE pro produkt MFT

Před instalací modulu pro protokolování databáze produktu Java EE postupujte podle těchto pokynů a připravte prostředí produktu Managed File Transfer .

Informace o této úloze

Další informace o registrátoru databáze Java EE naleznete v tématu “Konfigurace modulu protokolování MFT” na stránce 695.

Postup

1. Nainstalujte svůj databázový software pomocí dokumentace pro vaši databázi.

   Je-li podpora JDBC pro vaši databázi volitelnou komponentou, musíte nainstalovat tuto komponentu.
2. Vytvořte databázi pomocí nástrojů poskytnutých vaší databází. Databáze musí mít velikost stránky tabulkového prostoru a velikost stránky fondu vyrovnávacích pamětí alespoň 8K.

   Výchozí název schématu je FTELOG. Pokud používáte jiný název schématu než FTELOG, musíte upravit poskytnutý soubor SQL odpovídající vaší databázi, `ftelog_tables_db2.sql` nebo `ftelog_tables_oracle.sql`, aby se tak odrazil, než budete pokračovat dalším krokem.
3. Vytvořte požadované databázové tabulky pomocí nástrojů databáze.

   Multi V systému Multiplatformsobsahují soubory `ftelog_tables_db2.sql` a `ftelog_tables_oracle.sql` příkazy SQL, které lze spustit pro vytvoření tabulek.

   z/OS V systému z/OSzávisí soubor, který je třeba spustit, na verzi produktu Db2 for z/OS , kterou používáte:

   - Pro Db2 for z/OS 9.0 a starší spusťte soubor `ftelog_tables_zos.sql` , abyste vytvořili tabulky. Tento soubor vytváří tabulky s použitím datového typu INTEGER pro pole, která označují velikost přenesených souborů a ID tabulky přidružené k jednotlivým přenosům.
   - Pro produkt Db2 for z/OS 9.1 a novější spusťte soubor `ftelog_tables_zos_bigint.sql` pro vytvoření tabulek. Tento soubor vytváří tabulky s datovým typem BIGINT pro pole, která označují velikost přenesených souborů a ID tabulky přidružené k jednotlivým přenosům.
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 produkt MFT” na stránce 710.
5. Vytvořte frontu odmítnutí v produktu IBM MQ.

   Protože modul protokolování nikdy nevyřadí zprávy protokolu, pokud modul protokolování narazí na zprávu, kterou nedokáže zpracovat, umístí zprávu do fronty odmítnutí pro prozkoumání a možné opětovné zpracování. Pro tento účel nepoužívejte frontu nedoručených zpráv správce front, protože

odmítnuté zprávy nemají záhlaví DLH a protože odmítnuté zprávy nesmí být zkombinovány se zprávami vkládané do fronty nedoručených zpráv z jiných důvodů. Příkaz **fteCreateLogger** vytváří frontu odmítnutí. Výchozí název této fronty odmítnutí je SYSTEM.FTE.LOG.RJCT.*název_modulu_protokolování*

6. Postupujte podle pokynů v tématu "Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro produkt MFT" na stránce 720.

Jak pokračovat dále

Nyní můžete nainstalovat modul protokolování databáze produktu Java EE do aplikačního serveru vyhovujícího produktu Java EE. Postupujte podle pokynů v následujících tématech na základě aplikačního serveru, který používáte:

- "Instalace modulu protokolování databáze Java EE pro produkt MFT s produktem WebSphere Application Server 7.0" na stránce 712
- "Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT s produktem WebSphere Application Server Community Edition" na stránce 716

Změna názvu schématu v modulu protokolování databáze Java EE pro produkt MFT

Modul pro protokolování databáze Java Platform, Enterprise Edition (Java EE) může používat databázi, která má jiný než výchozí název schématu. Název schématu je třeba změnit v souboru EAR modulu protokolování databáze produktu Java EE .

Informace o této úloze

Chcete-li změnit název schématu, které modul protokolování databáze produktu Java EE používá, postupujte takto:

Postup

1. Extrahujte soubor JAR rozhraní JPA ze souboru EAR pomocí následujícího příkazu:

   ```
   jar -xvf ear_file lib/jpa_file
   ```

   kde:

   - Hodnota *soubor_EAR* je `com.ibm.wmqfte.databaselogger.jee.oracle.ear` nebo `com.ibm.wmqfte.databaselogger.jee.ear` podle toho, zda používáte produkt 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 rozhraní 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` tak, aby se změnil následující řádek:

   ```
   <property name="openjpa.jdbc.Schema" value="schema_name" />
   ```

   kde:

   - *schema_name* je název schématu, který chcete použít.
4. Aktualizujte soubor JAR JPA se změněným souborem `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 upraveným souborem JAR rozhraní JPA pomocí následujícího příkazu:

```
jar -uvf ear_file lib/jpa_file
```

kde:

- Hodnota *soubor_EAR* je `com.ibm.wmqfte.databaselogger.jee.oracle.ear` nebo `com.ibm.wmqfte.databaselogger.jee.ear` podle toho, zda používáte produkt 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

K instalaci modulu pro protokolování databáze Java EE použijte upravený soubor EAR.

Související úlohy

“Instalace modulu protokolování databáze Java EE pro produkt MFT s produktem WebSphere Application Server 7.0” na stránce 712

Postupujte podle těchto pokynů, chcete-li instalovat a konfigurovat modul protokolování databáze produktu Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s produktem WebSphere Application Server 7.0.

“Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT s produktem WebSphere Application Server Community Edition” na stránce 716

Postupujte podle těchto pokynů, chcete-li instalovat a konfigurovat modul protokolování databáze produktu Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s produktem WebSphere Application Server Community Edition.

Nastavení cesty k nativní knihovně v produktu WebSphere Application Server 7.0

Pokud implementujete aplikaci modulu protokolování Java Platform, Enterprise Edition (Java EE) do produktu WebSphere Application Server 7.0a chcete použít připojení režimu vazeb mezi aplikací a produktem IBM MQ, musíte nakonfigurovat poskytovatele systému zpráv produktu IBM MQ s umístěním nativních knihoven produktu IBM MQ v systému.

Informace o této úloze

Pokud nenastavíte cestu k nativní knihovně na svém aplikačním serveru, můžete v protokolu systému WebSphere Application Server 7.0 obdržet následující chybovou zprávu:

```
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 produktu WebSphere Application Server 7.0 proveďte následující kroky:

Postup

1. V navigačním podokně rozbalte položku **Prostředky** > **JMS** > **Poskytovatelé služby JMS**.
2. Vyberte poskytovatele systému zpráv produktu IBM MQ , který je ve správném rozsahu pro továrnu připojení nebo specifikaci aktivace, která vytváří připojení v režimu vázání.

   Poznámka: Nativní informace o cestě v rozsahu `Server` se používají přednostně k informacím o nativní cestě ve vyšším rozsazích a nativní informace o cestě v rozsahu `Node` se používají jako předvolba pro informace o nativní cestě v rozsahu `Cell` .

3. V části Obecné vlastnosti zadejte do pole **Cesta k nativní knihovně** úplný název adresáře, který obsahuje nativní knihovny produktu IBM MQ .

   Například na Linux zadejte `/opt/mqm/java/lib`. Zadejte pouze jeden název adresáře.
4. Klepněte na tlačítko **OK**.
5. Restartujte aplikační server, abyste obnovili konfiguraci.
6. Požadované: Restartujte aplikační server podruhé, abyste načetli knihovny.

Instalace modulu protokolování databáze Java EE pro produkt MFT s produktem WebSphere Application Server 7.0

Postupujte podle těchto pokynů, chcete-li instalovat a konfigurovat modul protokolování databáze produktu Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s produktem WebSphere Application Server 7.0.

Než začnete

Před instalací aplikace modulu protokolování databáze JEE postupujte podle pokynů v tématech "Příprava na instalaci modulu protokolování databáze Java EE pro produkt MFT" na stránce 709 a "Nastavení cesty k nativní knihovně v produktu WebSphere Application Server 7.0" na stránce 711.

Informace o této úloze

Další informace o registrátoru databáze Java EE viz "Konfigurace modulu protokolování MFT" na stránce 695.

Postup

1. Nastavte poskytovatele JDBC XA:
   a) Vyberte volbu **Prostředky** > **JDBC** > **PoskytovateléJDBC** z navigace administrativní konzoly produktu WebSphere Application Server 7.0 .
   b) Vytvořte poskytovatele JDBC pomocí průvodce konzoly klepnutím na volbu **Nový**.
   c) V kroku 1 v průvodci vyberte databázi, kterou používáte ze seznamu **Typ databáze** , a přidružený typ poskytovatele ze seznamu **Typ poskytovatele** . Ze seznamu **Typ implementace** vyberte volbu **Zdroj dat XA**. Klepněte na tlačítko **Další**.
   d) V kroku 2 tohoto průvodce zkontrolujte, zda je umístění adresáře s požadovanými soubory JAR databáze správně nastaveno. Klepněte na tlačítko **Další**.
   e) Klepnutím na tlačítko **Dokončit** na souhrnné stránce vytvořte poskytovatele JDBC .
2. Vytvořit aliasy ověřování. Vytvoříte jeden alias pro zdroj dat a druhý pro produkt IBM MQ:
   a) Vyberte volbu **Zabezpečení** > **Globální zabezpečení** z navigace administrativní konzoly produktu WebSphere Application Server 7.0 .
   b) Pod hlavičkou **Ověření** rozbalte volbu **Služba JAAS (Java Authentication and Authorization Service)**.
   c) Klepněte na volbu **Data ověřováníJ2C**. Otevře se stránka aliasu ověřování.
   d) Vytvořte alias ověřování pro váš zdroj dat:
      i) Klepněte na volbu **Nový**.
      ii) Zadejte podrobnosti pro **Alias**, **ID uživatele**, **Heslo**a **Popis**. Podrobnosti, které jsou zadány do polí **ID uživatele** a **Heslo** , se musí shodovat s podrobnostmi, které jste zadali při vytvoření uživatele databáze. Další informace naleznete v části "Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro produkt MFT" na stránce 720.
      iii) Klepněte na tlačítko **OK**.
   e) Vytvořte alias ověřování pro produkt IBM MQ:
      i) Klepněte na volbu **Nový**.

ii) Zadejte podrobnosti pro **Alias**, **ID uživatele**, **Heslo**a **Popis**. Podrobnosti, které jsou zadány do polí **ID uživatele** a **Heslo** , se musí shodovat s nastavením vašeho uživatele a hesla pro instalaci produktu IBM MQ .

iii) Klepněte na tlačítko **OK**.

3. Vytvořte zdroj dat:
   a) Vyberte volbu **Prostředky** > **JDBC** > **Zdroje dat** z navigace administrativní konzoly produktu WebSphere Application Server 7.0 .
   b) Vyberte rozevírací seznam **Rozsah** a změňte rozsah na příslušnou hodnotu. Například `Node=yourNode, Server=yourServer`.
   c) Vytvořte zdroj dat pomocí průvodce konzoly klepnutím na volbu **Nový**.
   d) V kroku 1 v průvodci 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 použijte rozevírací seznam **Vybrat existující poskytovatele JDBC** a vyberte poskytovatele JDBC vytvořeného v předchozích krocích. Klepněte na tlačítko **Další**.
   f) **Db2:** V kroku 3 v průvodci 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 adresu URL pro připojení do pole **Adresa URL** a zvolte správný pomocník datového úložiště v poli **Název pomocné třídy datového úložiště** .

      Oracle RAC: Při připojování k produktu Oracle Real Application Cluster musí adresa URL připojení obsahovat informace o hostiteli, které jsou nezbytné pro připojení ke všem dostupným instancím databáze.
   h) V kroku 4 v průvodci vyberte název aliasu ověřování zdroje dat, který jste definovali v kroku 2d , ze seznamu **Alias ověřování pro zotavení XA** . Vyberte stejný název v seznamech **Alias ověřování spravovaného komponentou** a **Alias ověřování spravovaný kontejnerem** .
   i) Klepněte na tlačítko **Dokončit** na souhrnné stránce, abyste vytvořili zdroj dat.
4. Volitelné: Ověřte konfiguraci zdroje dat:
   a) Vyberte volbu **Prostředky** > **JDBC** > **Zdroje dat** z navigace administrativní konzoly produktu WebSphere Application Server 7.0 .
   b) Klepněte na tlačítko **Testovat připojení** .
5. Vytvoření tématu.
   a) V navigaci administrativní konzoly produktu WebSphere Application Server 7.0 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 **Poskytovatel systému zpráv produktuIBM MQ**.
   e) Na panelu **Administrace** na stránce 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** zadejte `SYSTEM.FTE/Log/#` do pole **Název tématu** .
6. Vytvořte specifikaci aktivace:
   a) V navigačním stromu administrativní konzoly produktu WebSphere Application Server 7.0 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 **Poskytovatel systému zpráv produktuIBM MQ**.

e) V kroku 1 v průvodci zvolte jedinečné hodnoty pro pole **Název** a **Název rozhraní JNDI** , na které budete později znovu odkazovat v konfiguraci.

f) V kroku 1.1zadejte název rozhraní JNDI pro téma, které jste nastavili v kroku 5, v poli **Název cílového rozhraní JNDI** .

g) Ze seznamu **Typ cíle** vyberte volbu **Téma**.

h) V kroku 1.2 průvodce vyberte volbu **Trvalý odběr**. Do pole **Název odběru** zadejte `SYSTEM.FTE.DATABASELOGGER.AUTO` .

i) V kroku 2 v průvodci vyberte **Zadat všechny požadované informace do tohoto průvodce**.

j) V kroku 2.1zadejte požadovaný název správce front do pole **Název správce front nebo skupiny sdílení front** .

k) V kroku 2.2vyberte zvolenou metodu přenosu ze seznamu **Přenos** . Vyberete-li volbu **Vazby**, nebudou vyžadovány žádné další informace. Pokud vyberete volbu **Klient** nebo **Vazby, pak klient**, zadejte podrobnosti do pole **Název hostitele**, **Por**ta **Kanál připojení serveru**.

l) Volitelné: Klepnutím na volbu **Test připojení** potvrďte, že je správce front přítomen. Můžete však očekávat přijetí produktu `NOT_AUTHORIZED` , dokud se 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 vašeho připojení IBM MQ v poli **ID klienta** . Tento krok musíte dokončit nebo vaše připojení bude odmítnuto produktem IBM MQ s kódem chyby produktu `JMSCC0101` .

o) Pokud jste jako metodu přenosu zvolili položku **Klient** , posuňte se 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 **Spotřebitel připojení** na panelu **Rozšířené vlastnosti** zadejte 1 do pole **Maximální počet relací serveru** .

Poznámka: Před pokračováním se ujistěte, že jste dokončili tento krok. Pokud tak neučiníte, může modul protokolování selhat, aby fungoval správně.

r) V sekci **Další vlastnosti** na kartě **Konfigurace** klepněte na volbu **Rozšířené vlastnosti**. Nastavte hodnotu parametru **Zastavit koncový bod při selhání doručení zprávy** na minimu produktu 1.

Je-li hodnota vlastnosti _numberOfFailedAttemptsBeforeReject nastavena na více než 1 (viz 9j), nastavte parametr **Zastavit koncový bod při selhání doručení zprávy** alespoň na hodnotu vlastnosti _numberOfFailedAttemptsBeforeReject . Tím zabráníte zastavení koncového bodu, když je přijata zpráva, kterou nelze zpracovat (například nesprávně utvořená zpráva protokolu přenosu). Další informace naleznete v tématu Obsluha chyb modulu protokolování produktuMFT a odmítnutí.

7. Vytvořte továrnu připojení fronty.

a) V navigaci administrativní konzoly produktu WebSphere Application Server 7.0 klepněte na volbu **Prostředky** > **Služba 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 **Poskytovatel systému zpráv produktuIBM MQ**.

e) V kroku 1 v průvodci zvolte jedinečné hodnoty pro pole **Název** a **Název rozhraní JNDI** , na které budete později znovu odkazovat v konfiguraci.

f) V kroku 2 vyberte **Zadat všechny požadované informace do tohoto průvodce**.

g) V kroku 2.1zadejte požadovaný název správce front do pole **Název správce front nebo skupiny sdílení front** .

h) V kroku 2.2vyberte zvolenou metodu přenosu ze seznamu **Přenos** . Vyberete-li volbu **Vazby**, nebudou vyžadovány žádné další informace. Pokud vyberete volbu **Klient** nebo **Vazby, pak klient**, zadejte podrobnosti do pole **Název hostitele**, **Port**a **Kanál připojení serveru**.

i) Volitelné: Klepnutím na volbu **Test připojení** potvrďte, že je správce front přítomen. Můžete však očekávat, že obdržíte `NOT_AUTHORIZED` , dokud se neodkazujete na alias ověřování v kroku 7h.

j) Pokud jste jako metodu transportu vybrali volbu **Klient** nebo **Vazby a poté klienta** , 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 , z seznamů **Alias ověřování pro zotavení XA** a **Alias ověřování spravovaný kontejnerem** .

8. Vytvořte frontu odmítnutí v produktu WebSphere Application Server:

a) V navigaci administrativní konzoly produktu WebSphere Application Server 7.0 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 **Poskytovatel systému zpráv produktuIBM MQ**.

e) Vyberte jedinečné hodnoty pro pole **Název** a **Název rozhraní JNDI** , na které budete později znovu odkazovat v konfiguraci.

f) Zadejte `SYSTEM.FTE.LOG.RJCT.`*`logger_name`* do pole **Název fronty** . Ujistěte se, že jste tuto frontu vytvořili ve svém koordinačním správci front.

g) Zadejte název správce front do pole **Název správce front** .

h) Klepněte na tlačítko **OK**.

9. Nainstalujte aplikaci modulu protokolování databáze JEE:

a) V administrativní konzole produktu WebSphere Application Server 7.0 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` v instalaci produktu Managed File Transfer Service
a klepněte na tlačítko **Další**.

e) Na následující obrazovce vyberte volbu **Podrobná** , chcete-li zobrazit všechny volby a parametry instalace, a klepněte na tlačítko **Další**.

f) Chcete-li přijmout výchozí hodnoty, klepněte na tlačítko **Další** prostřednictvím kroků průvodce 1 až 4.

g) V kroku 5 v průvodci **Vázat moduly listener pro objekty bean řízené zprávami**se posuňte na sekci **Vazby modulu listener** . Klepněte na volbu **Specifikace aktivace**.

Zadejte požadované hodnoty do následujících polí:

Název rozhraní JNDI cílového prostředku
Název rozhraní JNDI, který jste zadali při vytváření specifikace aktivace v kroku 6d.

Název rozhraní JNDI cíle
Název rozhraní JNDI, který jste zadali při vytváření tématu v kroku 5d.

Klepněte na tlačítko **Další**.

h) V kroku 6 v průvodci **Mapovat odkazy na prostředek na prostředky**zadejte podrobnosti do pole **Název rozhraní JNDI cílového prostředku** . Tento název je názvem rozhraní JNDI, které 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 názvem 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: Když se připojujete k produktu Oracle Real Application Cluster, musíte nastavit hodnotu vlastnosti _numberOfFailedAttemptsBeforeReject na **alespoň** 2. Tato vlastnost určuje, kolikrát se modul protokolování pokusí zpracovat zprávu auditu poté, co dojde k selhání. V případě překonání selhání databáze se pravděpodobně vyskytne alespoň jedno selhání. Chcete-li se vyhnout zbytečnému přesunu zprávy do fronty odmítnutí, umožní zvýšení této hodnoty provést druhý pokus o úspěch, který obvykle má za následek úspěch, protože je vytvořeno připojení k nové instanci databáze. Pokud zjistíte během testování, že zprávy jsou stále přesunuty do fronty odmítnutí během překonání selhání instance databáze, zvyšte tuto hodnotu dále: načasování přepnutí mezi instancemi může způsobit více než jedno selhání pro stejnou zprávu. Avšak mějte na paměti, že zvýšení této hodnoty ovlivní všechny případy selhání (například deformovaná zpráva) a nikoli pouze překonání selhání databáze, takže zvyšte hodnotu opatrně, abyste se vyvarovali zbytečným opakovaní.

k) V kroku 9 v průvodci, **Metadata pro moduly**klepněte na tlačítko **Další**.

l) V kroku 10 v průvodci **Souhrn**klepněte na tlačítko **Dokončit**.

10. Nyní můžete spustit aplikaci z administrativní konzoly produktu WebSphere Application Server 7.0 :

a) Z navigace konzoly vyberte volbu **Aplikace** > **Typy aplikací** > **Podnikové aplikace platformyWebSphere** .

b) Vyberte zaškrtávací políčko pro podnikovou aplikaci **Zapisovač protokolu** z tabulky kolekcí a klepněte na tlačítko **Spustit**.

Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT s produktem WebSphere Application Server Community Edition

Postupujte podle těchto pokynů, chcete-li instalovat a konfigurovat modul protokolování databáze produktu Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer s produktem WebSphere Application Server Community Edition.

Než začnete

Před instalací aplikace modulu protokolování databáze Java EE postupujte podle pokynů uvedených v tématu “Příprava na instalaci modulu protokolování databáze Java EE pro produkt MFT” na stránce 709.

Informace o této úloze

Další informace o registrátoru databáze Java EE naleznete v tématu “Konfigurace modulu protokolování MFT” na stránce 695.

Postup

1. Naimplementujte adaptér prostředků produktu IBM MQ , `wmq.jmsra.rar`.

- Chcete-li implementovat adaptér prostředků produktu IBM MQ pro modul protokolování databáze produktu Java EE pomocí koordinačního správce front QM_JUPITER, proveďte následující kroky. Tento příklad platí, je-li instance produktu WebSphere Application Server Community Edition spuštěna na stejném systému jako správce front produktu IBM MQ , ke kterému se chcete připojit.

  a. Vytvořte soubor s plánem, který definuje připojení ke koordinačnímu správci front produktu MFT . Následující příklad souboru s plánem definuje připojení ke správci front s názvem QM_JUPITER a odkazuje na frontu s názvem SYSTEM.FTE.LOG.RJCT.LOGGER1 na daném správci front.

```
<?xml version="1.0" encoding="UTF-8"?>
<connector xmlns="http://geronimo.apache.org/xml/ns/j2ee/connector">
  <resourceadapter>
    <resourceadapter-instance>
      <resourceadapter-name>WMQ</resourceadapter-name>
```

```
      <workmanager>
        <gbean-link>DefaultWorkManager</gbean-link>
      </workmanager>
    </resourceadapter-instance>
    <outbound-resourceadapter>
      <connection-definition>
        <connectionfactory-interface>javax.jms.ConnectionFactory</connectionfactory-interface>
        <connectiondefinition-instance>
          <name>jms/WMQFTEJEEDBLoggerRejectQueueCF</name>
          <config-property-setting name="queueManager">QM_JUPITER</config-property-setting>
          <config-property-setting name="transportType">BINDINGS</config-property-setting>
          <connectionmanager>
            <xa-transaction>
              <transaction-caching/>
            </xa-transaction>
            <single-pool>
              <max-size>10</max-size>
              <min-size>1</min-size>
              <blocking-timeout-milliseconds>5000</blocking-timeout-milliseconds>
              <idle-timeout-minutes>2</idle-timeout-minutes>
              <match-all />
            </single-pool>
          </connectionmanager>
        </connectiondefinition-instance>
      </connection-definition>
    </outbound-resourceadapter>
  </resourceadapter>
  <adminobject>
    <adminobject-interface>javax.jms.Queue</adminobject-interface>
    <adminobject-class>com.ibm.mq.connector.outbound.MQQueueProxy</adminobject-class>
    <adminobject-instance>
      <message-destination-name>jms/WMQFTEJEEDBLoggerRejectQueue</message-destination-name>
      <config-property-setting name="baseQueueManagerName">QM_JUPITER</config-property-setting>
      <config-property-setting name="baseQueueName">SYSTEM.FTE.LOG.RJCT.LOGGER1</config-property-setting>
    </adminobject-instance>
  </adminobject>
</connector>
```

Chcete-li použít tento soubor plánu ve vašem prostředí, změňte název správce front QM_JUPITER na název koordinačního správce front.

b. Otevřete administrativní konzolu produktu WebSphere Application Server CE.

c. V seznamu **Obecné akce konzoly** na **Úvodní stránce**klepněte na volbu **Implementovat nové aplikace** > **Implementovat nový**.

d. Do pole **Archiv** zadejte *mq_install_root*/java/lib/jca/wmq.jmsra.rar

e. Do pole **Plán** zadejte cestu k souboru s plánem, který jste vytvořili v kroku 1a.

- Pokud je instance produktu WebSphere Application Server Community Edition spuštěna na jiném systému pro správce front produktu IBM MQ , ke kterému se chcete připojit, proveďte následující kroky pro implementaci adaptéru prostředků produktu IBM MQ .

  a. Vytvořte soubor s plánem, který definuje připojení ke koordinačnímu správci front produktu WMQFTE. Následující příklad souboru s plánem definuje připojení ke správci front QM_SATURN, který je umístěn v jiném systému než instalace produktu WebSphere Application Server Community Edition , a odkaz na frontu s názvem SYSTEM.FTE.LOG.RJCT.LOGGER1 na daném správci front. Název hostitele QM_SATURN je `saturn.example.com`. Port QM_SATURN je 1415. Kanál QM_SATURN je SYSTEM.DEF.SVRCONN.

     Vzhledem k tomu, že aplikační server a správce front se nacházejí v různých systémech, je třeba ke správci front použít připojení v režimu klienta. Následující soubor plánu nastaví hodnotu prvku `<config-property-setting>` , který má název `transportType` na CLIENT.

```
<?xml version="1.0" encoding="UTF-8"?>
<connector xmlns="http://geronimo.apache.org/xml/ns/j2ee/connector">
  <resourceadapter>
    <resourceadapter-instance>
      <resourceadapter-name>WMQ</resourceadapter-name>
      <workmanager>
        <gbean-link>DefaultWorkManager</gbean-link>
      </workmanager>
    </resourceadapter-instance>
    <outbound-resourceadapter>
      <connection-definition>
```

```
        <connectionfactory-interface>javax.jms.ConnectionFactory</connectionfactory-interface>
        <connectiondefinition-instance>
          <name>jms/WMQFTEJEEDBLoggerRejectQueueCF</name>
          <config-property-setting name="queueManager">QM_SATURN</config-property-setting>
          <config-property-setting name="transportType">CLIENT</config-property-setting>
          <config-property-setting name="channel">SYSTEM.DEF.SVRCONN</config-property-setting>
          <config-property-setting name="hostName">saturn.example.com</config-property-setting>
          <config-property-setting name="port">1415</config-property-setting>
          <connectionmanager>
            <xa-transaction>
              <transaction-caching/>
            </xa-transaction>
            <single-pool>
              <max-size>10</max-size>
              <min-size>1</min-size>
              <blocking-timeout-milliseconds>5000</blocking-timeout-milliseconds>
              <idle-timeout-minutes>2</idle-timeout-minutes>
              <match-all />
            </single-pool>
          </connectionmanager>
        </connectiondefinition-instance>
      </connection-definition>
    </outbound-resourceadapter>
  </resourceadapter>
  <adminobject>
    <adminobject-interface>javax.jms.Queue</adminobject-interface>
    <adminobject-class>com.ibm.mq.connector.outbound.MQQueueProxy</adminobject-class>
    <adminobject-instance>
      <message-destination-name>jms/WMQFTEJEEDBLoggerRejectQueue</message-destination-name>
      <config-property-setting name="baseQueueManagerName">QM_SATURN</config-property-setting>
      <config-property-setting name="baseQueueName">SYSTEM.FTE.LOG.RJCT.LOGGER1</config-property-setting>
    </adminobject-instance>
  </adminobject>
</connector>
```

Chcete-li použít tento soubor plánu ve vašem prostředí, změňte správce front QM_SATURN na název koordinačního správce front. Změňte hodnotu názvu hostitele, portu a kanálu na hodnoty pro koordinačního správce front.

b. Zkopírujte soubor *mq_install_root*/java/lib/jca/wmq.jmsra.rar ze systému, kde je nainstalován produkt IBM MQ , do systému, kde je nainstalován produkt WebSphere Application Server CE.

c. Otevřete administrativní konzolu produktu WebSphere Application Server CE.

d. V seznamu **Obecné akce konzoly** na **Úvodní stránce**klepněte na volbu **Implementovat nové aplikace** > **Implementovat nový**.

e. V poli **Archiv** zadejte cestu ke kopii souboru wmq.jmsra.rar , kterou jste získali.

f. Do pole **Plán** zadejte cestu k souboru s plánem, který jste vytvořili.

2. Musíte definovat konektor databáze, aby měla aplikace modulu protokolování databáze produktu Java EE přístup k požadované databázi z prostředí produktu WebSphere Application Server Community Edition .

   Proveďte následující kroky z administrativní konzoly produktu WebSphere Application Server Community Edition :

   a) V závislosti na úrovni produktu WebSphere Application Server Community Edition , kterou používáte, v **Navigaci konzoly** buď vyberte volbu **Služby** > **Fondy databází**, nebo vyberte volbu **Prostředky** > **Zdroje dat**.

   b) Vytvořte fond databází pomocí průvodce fondem databáze Geronimo. Do pole **Název fondu databáze** zadejte jdbc/wmqfte-database.

   c) Pro volbu **Typ databáze** vyberte volbu DB2 XA nebo Oracle Thin, podle vhodnosti pro databázi.

   d) Klepněte na tlačítko **Další**.

   e) V poli **Soubor jar ovladače** vyberte odpovídající soubor JAR pro vaši databázi.

   f) Do pole **Název databáze** zadejte název databáze, ke které se připojujete, pro informace o stavu přenosu.

   g) Do pole **Jméno uživatele** zadejte jméno uživatele pro připojení k databázi a ověření s ní.

   h) V polích **Heslo** a **Potvrdit heslo** zadejte heslo pro ověření s databází.

i) Do pole **Číslo portu** zadejte číslo portu, které používáte, pokud se nejedná o výchozí port.

j) Ujistěte se, že hodnota pro **Typ ovladače** je 4.

k) Vyberte položku XA ze seznamu **Typ transakce** .

l) Klepněte na tlačítko **Implementovat**.

3. Update the Managed File Transfer Java EE database logger application `openejb-jar.xml` file for your environment. Použijte obslužný program jar sady SDK produktu Java k provedení následujících kroků:

   a) Extrahujte soubor JAR sady EJB ze zadaného souboru EAR spuštěním následujícího příkazu:

   ```
   jar -xf ear_file_name com.ibm.wmqfte.databaselogger.jee.ejb.jar
   ```

   kde parametr *název_souboru_ear* je `com.ibm.wmqfte.databaselogger.jee.ear` nebo `com.ibm.wmqfte.databaselogger.jee.oracle.ear` podle toho, zda používáte produkt Db2 nebo Oracle. Soubor EAR je umístěn v adresáři *MQ_INSTALLATION_PATH*`/mqft/web` v instalaci serveru IBM WebSphere MQ File Transfer Edition .

   b) Extrahujte soubor `META-INF/openejb-jar.xml` z dříve extrahovaného souboru JAR sady EJB, `com.ibm.wmqfte.databaselogger.jee.ejb.jar`, spuštěním následujícího příkazu:

   ```
   jar -xf com.ibm.wmqfte.databaselogger.jee.ejb.jar META-INF/openejb-jar.xml
   ```

   c) Použijte textový editor k úpravě extrahovaného souboru `META-INF/openejb-jar.xml` . Změňte následující hodnoty `activation-config-property` tak, aby odpovídaly vašemu prostředí:

   queueManager
   Název správce front produktu IBM MQ používaného modulem protokolování databáze produktu Java EE .

   hostName
   Název hostitele, který má být použit pro připojení k zadanému správci front IBM MQ . Tato hodnota není vyžadována, pokud se připojujete ke správci front v režimu vazeb.

   transportType
   Zda se má připojit k zadanému správci front IBM MQ v režimu klienta nebo vazeb.

   Port
   Není vyžadováno, pokud jste zadali **`transportType`** vazeb. Port, který má být použit pro připojení k určenému správci front IBM MQ .

   kanál
   Není vyžadováno, pokud jste zadali **`transportType`** vazeb. Kanál serveru, který má být použit pro připojení k určenému správci front IBM MQ .

   d) Aktualizujte soubor JAR sady EJB se změněným souborem `META-INF/openejb-jar.xml` spuštěním následujícího příkazu:

   ```
   jar -uf com.ibm.wmqfte.databaselogger.jee.ejb.jar META-INF/openejb-jar.xml
   ```

   e) Aktualizujte dodaný soubor EAR s aktualizovaným souborem JAR sady EJB spuštěním následujícího příkazu:

   ```
   jar -uf ear_file_name com.ibm.wmqfte.databaselogger.jee.ejb.jar
   ```

   kde parametr *název_souboru_ear* je `com.ibm.wmqfte.databaselogger.jee.ear` nebo `com.ibm.wmqfte.databaselogger.jee.oracle.ear` v závislosti na vaší databázi.

4. Chcete-li nasadit soubor EAR na aplikační server, proveďte následující kroky z administrativní konzoly produktu WebSphere Application Server Community Edition .

   a) Vyberte volbu: **Aplikace** > **Implementovat nový** z nabídky **Navigace konzoly** .

b) Do pole **Archiv** zadejte soubor EAR: `com.ibm.wmqfte.databaselogger.jee.ear` nebo `com.ibm.wmqfte.databaselogger.jee.oracle.ear` v závislosti na vaší databázi.

c) Ponechte pole **Plán** prázdné.

d) Ujistěte se, že je zaškrtnuto políčko **Spustit aplikaci po instalaci** .

e) Klepněte na volbu **Instalovat**. Aplikace modulu protokolování databáze JEE je nainstalována a spuštěna.

Konfigurace uživatelského přístupu pro modul protokolování databáze Java EE pro produkt MFT

Když konfigurujete modul protokolování databáze Java Platform, Enterprise Edition (Java EE) pro produkt Managed File Transfer, potřebujete uživatelské účty pro přístup k databázi IBM MQ, k databázi a k operačnímu systému. Počet uživatelů operačního systému, které se požadují, 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 systémů, které používáte. Uživatelské účty jsou nezbytné pro přístup k následujícím třem prostředím:

- Lokální operační systém
- IBM MQ
- Databáze

Můžete nainstalovat modul protokolování databáze JEE, IBM MQ a vaši databázi na jednom systému nebo na více systémech. Tyto komponenty lze instalovat v následujících ukázkových topologiích:

Modul protokolování databáze produktu Java EE , produkt IBM MQa všechny databáze na stejném systému
: Můžete definovat jediného uživatele operačního systému pro použití se všemi třemi komponentami. Modul protokolování používá režim vazeb pro připojení k databázi IBM MQ a nativní připojení pro připojení k databázi.

Modul protokolování databáze Java EE a produkt IBM MQ na jednom systému, databáze na samostatném systému.
: Vytvoříte dva uživatele pro tuto konfiguraci: uživatel operačního systému na systému, na kterém běží modul protokolování, a uživatel operačního systému se vzdáleným přístupem k databázi na databázovém serveru. Modul protokolování používá režim vazeb pro připojení k databázi IBM MQ a připojení klienta pro přístup k databázi.

Java EE logger databáze na jednom systému, IBM MQ na jiném systému, databáze na dalším systému
: Pro tuto konfiguraci vytvoříte tři uživatele: uživatel operačního systému pro spuštění aplikačního serveru, uživatele produktu IBM MQ pro přístup k používaným frontám a tématům a uživateli databázového serveru k přístupu a vkládání do tabulek databáze. Modul protokolování používá klientský režim pro přístup k databázi IBM MQ a připojení klienta pro přístup k databázi.

Jako příklad předpokládejme, že zbytek těchto pokynů předpokládá, že se uživatel nazývá `ftelog`, ale můžete použít libovolné jméno uživatele, nové nebo existující. Nakonfigurujte oprávnění uživatele následujícím způsobem:

Postup

1. Ujistěte se, že uživatel operačního systému má svou vlastní skupinu a že také není ve všech skupinách s povoleními na koordinačním správci front v režimu wide-sarand. Uživatel by neměl být ve skupině mqm. Na určitých platformách má skupina personálu automaticky také přístup správce front; uživatel modulu protokolování by neměl být ve skupině zaměstnanců. Můžete zobrazit záznamy oprávnění pro samotný správce front a pro objekty v něm obsažené v produktu IBM MQ Explorer. Klepněte pravým tlačítkem myši na objekt a vyberte volbu **Oprávnění k objektu > Správa záznamů oprávnění**.

Na příkazovém řádku můžete použít příkazy dspmqaut (display authority) nebo dmpmqauth (dump authority).

2. Použijte okno **Spravovat záznamy oprávnění** v produktu IBM MQ Explorer nebo příkaz setmqaut (grant nebo revoke authority) , abyste přidali oprávnění pro vlastní skupinu uživatele IBM MQ (v systému UNIXjsou oprávnění k produktu IBM MQ přidružena pouze ke skupinám, nikoli k jednotlivým uživatelům). Požadované orgány jsou následující:
   - CONNECT a INQUIRE na správci front (knihovny produktu IBM MQ Java vyžadují oprávnění INQUIRE k provozu).
   - Oprávnění SUBSCRIBE v systému SYSTEM.FTE .
   - Oprávnění PUT na SYSTEM.FTE.LOG.RJCT.*název_modulu_protokolování* .

   Jako výchozí názvy jsou použity výchozí názvy fronty odmítnutí a příkazu. Pokud jste při konfiguraci front modulu protokolování vybrali různé názvy front, přidejte místo nich oprávnění k těmto názvům front.
3. Proveďte konfiguraci uživatele databáze, která je specifická pro databázi, kterou používáte.
   - Pokud je vaše databáze Db2, proveďte následující kroky:

     Poznámka: Pro správu uživatelů databází pomocí produktu Db2existuje několik mechanizmů. Tyto pokyny se vztahují na výchozí schéma založené na uživatelích operačního systému.

     – Ujistěte se, že uživatel produktu `ftelog` není ve všech administračních skupinách produktu Db2 (například db2iadm1, db2fadm1nebo dasadm1).

     – Udělte uživateli oprávnění k připojení k databázi a oprávnění k výběru, vložení a aktualizaci tabulek, které jste vytvořili jako součást kroku 2: vytvoření požadovaných databázových tabulek.
   - Je-li vaše databáze Oracle, proveďte následující kroky:

     – Ujistěte se, že uživatel `ftelog` není ve všech administračních skupinách Oracle (například ora_dba on Windows nebo dba na UNIX).

     – Udělte uživateli oprávnění k připojení k databázi a oprávnění pro výběr, vložení a aktualizaci tabulek, které jste vytvořili jako součást kroku 2: vytvoření požadovaných databázových tabulek.

Migrace zapisovače protokolu databáze Java EE

Chcete-li migrovat modul protokolování databáze Java EE na serveru WebSphere Application Server 7.0 z IBM WebSphere MQ File Transfer Edition 7.0 na IBM WebSphere MQ 7.5 nebo novější, postupujte takto:

Postup

1. Otevřete konzolu WebSphere Application Server .
2. Klepněte na volbu **Aplikace** > **Typy aplikací** > **Podnikové aplikace**. V seznamu aplikací vyhledejte aplikaci modulu protokolování databáze produktu IBM WebSphere MQ File Transfer Edition . Není-li aplikace modulu pro protokolování databáze již zastavena, vyberte aplikaci a klepněte na tlačítko **Zastavit**.
3. Poznamenejte si nastavení konfigurace, které jste dříve nastavili pro modul protokolování databáze JEE. Tyto informace budete potřebovat později v kroku “7” na stránce 722.
   a) Pokud jste původně provedli změny z výchozích nastavení pro moduly EJB při instalaci modulu protokolování databáze (další informace viz krok 9), klepněte na volbu **Podnikové aplikace** > **WebSphere MQ File Transfer Edition Database logger** > **Položky prostředí pro moduly EJB** a poznamenejte si nastavení v podokně.

   b) Klepněte na volbu **Podnikové aplikace** > **WebSphere MQ File Transfer Edition modul protokolování databáze** > **Vazby modulu listener objektu Message Driven Bean** a poznamenejte si použitou specifikaci aktivace, **Název rozhraní JNDI cílového prostředku** a **Název cílového rozhraní JNDI**.

   c) Klepněte na volbu **Podnikové aplikace** > **WebSphere MQ File Transfer Edition modul protokolování databáze** > **Odkazy na prostředky** a poznamenejte si podrobnosti o továrně připojení fronty odmítnutí.

d) Klepněte na volbu **Podnikové aplikace** > **WebSphere MQ File Transfer Edition modul protokolování databáze** > **Odkazy na položku prostředí prostředků** a poznamenejte si podrobnosti fronty odmítnutí.

4. Odinstalujte aplikaci modulu pro protokolování databáze produktu IBM WebSphere MQ File Transfer Edition klepnutím na volbu **Aplikace** > **Typy aplikací** > **Podnikové aplikace**. Vyberte aplikaci modulu pro protokolování databáze a klepněte na volbu **Odinstalovat**.
5. Volitelné: Pokud používáte více instalací k migraci na verzi produktu IBM WebSphere MQ 7.5nebo novější a cesta k nativní knihovně je odlišná, změňte cestu klepnutím na volbu **Prostředky** > **Poskytovatelé JMS** > **WebSphere MQ**

   Je-li například cesta k nativní knihovně: `C:\Program Files\IBM\WebSphere MQ\java\lib`, změňte cestu na: `C:\Program Files\IBM\`*`New MQ Installation Location`*`\java\lib`
6. Volitelné: Pokud používáte více instalací pro migraci do produktu IBM WebSphere MQ 7.5 nebo novější, musíte správce front přidružit k nové instalaci pomocí příkazu setmqm.
7. Znovu nainstalujte aplikaci modulu protokolování databáze s použitím informací v produktu “Instalace modulu protokolování databáze Java EE pro produkt MFT s produktem WebSphere Application Server 7.0” na stránce 712 a informací, které jste zaznamenali dříve v kroku “3” na stránce 721.
8. Spusťte nový modul pro protokolování databáze po klepnutí na volbu **Aplikace** > **Typy aplikací** > **Podnikové aplikace**. Vyberte aplikaci modulu pro protokolování databáze a klepněte na tlačítko **Spustit**.
9. Chcete-li ověřit migraci, zkontrolujte databázi, abyste se ujistili, že jsou záznamy zapisovány.

Migrace ze samostatného modulu protokolování databáze do modulu protokolování databáze Java EE pro produkt MFT

Můžete migrovat ze samostatného modulu protokolování databáze na modul protokolování databáze produktu Java EE . Je třeba zastavit samostatný modul protokolování databáze a nainstalovat modul protokolování databáze JEE. Chcete-li se vyhnout ztrátě nebo duplikaci záznamů protokolu, musíte zastavit publikování zpráv do SYSTEM.FTE před zastavením samostatného modulu pro protokolování databáze a po instalaci modulu pro protokolování databáze produktu Java EE jej restartujte. Před migrací zálohujte svou databázi.

Informace o této úloze

Postup

1. Před zastavením databáze spusťte na koordinačním správci front tento příkaz MQSC: `ALTER QM PSMODE(COMPAT)`

   Tím dojde k publikování zpráv, které jsou publikovány do SYSTEM.FTE/Log téma. Počkejte, až modul protokolování zpracuje všechny zprávy ve svém odběru. Při výchozím nastavení se tento odběr nazývá SYSTEM.FTE.LOGGER.AUTO.
2. Zastavte modul pro protokolování databáze pomocí příkazu **`fteStopLogger`** .
3. Zazálohujte databázi pomocí nástrojů dodaných s databázovým softwarem.
4. Odstraňte odběr náležející do samostatného modulu protokolování databáze.

   Při výchozím nastavení se tento odběr nazývá SYSTEM.FTE.LOGGER.AUTO.
5. Pokud se vaše schéma databáze nachází ve starší verzi, musíte schéma migrovat na každou následnou úroveň v daném pořadí. Je-li například vaše schéma databáze verze V7.0.1 a provádíte migraci na verzi V7.0.4, musíte své schéma migrovat z verze V7.0.1 na verzi V7.0.2a poté z verze V7.0.2 na V7.0.3a poté z verze V7.0.3 na V7.0.4. Proveďte migraci vašeho schématu 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 ní existující data. Další informace viz Migrace databázových tabulek na serveru Db2 v produktu z/OS na MQ V8.0 nebo novější.

- Pokud vaše databáze není Db2 nebo jste vytvořili databázi s velikostí stránky větší než 8K, můžete schéma migrovat stejným způsobem jako u jiných verzí provedením následujících kroků.
- Provádíte-li migraci mezi databázovými tabulkami za jakýchkoli jiných okolností, postupujte takto:
  a. Vyberte soubor, který odpovídá vaší databázové platformě, a který má název, který obsahuje řetězec *old-new*. Tento soubor je umístěn v adresáři *MQ_INSTALLATION_PATH*/mqft/sql v aplikaci Remote Tools and Documentation .
  b. Pokud jste provedli změny v počátečním schématu, zkontrolujte soubor migrace a ujistěte se, že soubor bude kompatibilní s upravenou databází.
  c. Spusťte soubor SQL pro vaši databázi.

6. Nainstalujte soubor EAR modulu protokolování databáze produktu Java EE .
7. Nasaďte modul protokolování databáze produktu Java EE . Další informace viz téma “Instalace modulu pro protokolování databáze produktu Java EE pro produkt MFT” na stránce 708.
8. Spusťte následující příkaz MQSC pro koordinačního správce front: `ALTER QMGR PSMODE(ENABLED)`
   Tím je umožněno publikování zpráv do SYSTEM.FTE/Log téma.

Výsledky

Konfigurace mostu produktu Connect:Direct

Nakonfigurujte most produktu Connect:Direct k přenosu souborů mezi sítí Managed File Transfer a sítí Connect:Direct . Komponenty mostu Connect:Direct jsou uzly produktu Connect:Direct a Managed File Transfer , které jsou vyhrazeny 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 UNIX.
- 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 produktu 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 produktu Connect:Direct .

Při výchozím nastavení agent mostu Connect:Direct používá protokol TCP/IP k připojení k uzlu produktu Connect:Direct . Pokud chcete zabezpečené připojení mezi vaším agentem mostu Connect:Direct a uzlem Connect:Direct , můžete použít protokol SSL nebo protokol TLS.

Postup

1. Zvolte operační systémy pro agenta mostu Connect:Direct a uzel:
   a) Zvolte systém, na kterém běží buď produkt Windows , nebo server Linux v systému x86-64 a nainstalujte agenta mostu Connect:Direct .
   b) Vyberte operační systém, který je podporován Connect:Direct pro Windows nebo Connect:Direct pro UNIX pro instalaci uzlu mostu Connect:Direct .
2. Zvolte a nakonfigurujte uzel produktu Connect:Direct :

   Než budete postupovat podle těchto pokynů, musíte mít nainstalovaný uzel produktu Connect:Direct .
   a) Zvolte uzel Connect:Direct , se kterým bude agent Managed File Transfer komunikovat.
   b) Zkontrolujte mapu sítě pro vybraný uzel produktu Connect:Direct . Pokud mapa sítě obsahuje nějaké položky pro vzdálené uzly spuštěné v operačním systému Windows , je třeba zajistit, aby tyto položky určily, že uzly jsou spuštěny v systému Windows.

      Windows Je-li uzel produktu Connect:Direct vybraný pro most produktu Connect:Direct spuštěn v systému Windows, použijte k úpravě mapy sítě klienta Connect:Direct . Ujistěte se, že pole **Operační systém** pro všechny vzdálené uzly, které jsou spuštěny na serveru Windows , je nastaveno na **Windows**.
3. Vytvořte a nakonfigurujte agenta mostu Connect:Direct :
   a) Vytvořte agenta mostu Connect:Direct pomocí příkazu **fteCreateCDAgent** .
      - Je třeba zadat hodnotu parametru **cdNode** . Tento parametr určuje název, který agent používá pro uzel produktu Connect:Direct , který je součástí mostu Connect:Direct . Použijte název uzlu Connect:Direct , který jste vybrali v předchozí sekci.
      - Poskytněte hodnoty pro parametry **cdNodeHost** a **cdNodePort** , které definují uzel Connect:Direct , se kterým agent komunikuje.

        Pokud nezadáte hodnotu parametru **cdNodeHost** , použije se název hostitele nebo IP adresa lokálního systému. Pokud nezadáte hodnotu pro argument **cdNodePort** , použije se hodnota 1363 .
      - Volitelně můžete použít informace v fteCreateAgent k určení, zda je třeba určit hodnotu pro parametr **cdTmpDir** .
   b) Mapujte pověření uživatele použitá produktem Managed File Transfer k pověření uživatele na uzlu produktu Connect:Direct . Pověření můžete mapovat pomocí jedné z následujících metod:
      - Vytvořte soubor `ConnectDirectCredentials.xml` , abyste definovali informace o mapování pověření. Další informace viz téma “Mapování pověření pro produkt Connect:Direct pomocí souboru ConnectDirectCredentials.xml” na stránce 725.
      - Napsat uživatelskou proceduru pro provedení mapování pověření pro váš most produktu Connect:Direct . Další informace viz téma “Mapování pověření pro produkt Connect:Direct pomocí tříd ukončení” na stránce 727.
4. Nakonfigurujte soubor `ConnectDirectNodeProperties.xml` tak, aby obsahoval informace o vzdálených uzlech produktu Connect:Direct :

   Než budete postupovat podle těchto pokynů, musíte mít vytvořeného agenta mostu produktu Connect:Direct .

   Upravte šablonu `ConnectDirectNodeProperties.xml` v konfiguračním adresáři agenta mostu Connect:Direct . Pro každý uzel Connect:Direct nebo skupinu uzlů, pro které chcete definovat informace, proveďte následující kroky:
   a) Uvnitř prvku nodeProperties vytvořte prvek node .

b) Přidejte atribut name do prvku node . Zadejte hodnotu tohoto atributu jako vzor, který bude odpovídat názvu jednoho nebo více vzdálených uzlů Connect:Direct .

c) Volitelné: Přidejte atribut pattern do prvku node , který uvádí, jaký typ vzoru má být hodnota v atributu name . Platné hodnoty jsou `regex` a `wildcard`. Standardní volba je `wildcard`.

d) Přidejte atribut type do prvku node , který určuje operační systém, který je určen vzdáleným uzlem Connect:Direct zadaným atributem name .

Platné jsou tyto hodnoty:

- `Windows` -uzel běží na systému Windows
- `UNIX` -uzel běží na UNIX nebo Linux
- z/OS `z/OS`, `zos`, `os/390`nebo `os390` -uzel je spuštěn v systému z/OS

Hodnota tohoto atributu není citlivá na velikost písmen. Přenosy do vzdálených uzlů v jiných operačních systémech most Connect:Direct nepodporuje.

5. Nakonfigurujte zabezpečené připojení mezi agentem mostu Connect:Direct a uzlem Connect:Direct .

Příklad tohoto postupu najdete v tématu Konfigurace zabezpečení SSL nebo TLS mezi agentem mostu Connect:Direct a uzlem Connect:Direct.

Mapování pověření pro produkt Connect:Direct

Namapujte pověření uživatele v produktu Managed File Transfer na pověření uživatele na uzlu produktu Connect:Direct pomocí výchozí funkce mapování pověření agenta mostu Connect:Direct nebo zadáním vlastní uživatelské procedury. Managed File Transfer poskytuje vzorovou uživatelskou proceduru, která provádí mapování pověření uživatele.

Mapování pověření pro produkt Connect:Direct pomocí souboru ConnectDirectCredentials.xml

Namapujte pověření uživatele v produktu Managed File Transfer na pověření uživatele v uzlech produktu Connect:Direct pomocí výchozí funkce mapování pověření agenta mostu produktu Connect:Direct . Managed File Transfer poskytuje soubor XML, který můžete upravit a zahrnout vaše informace o pověření.

Informace o této úloze

Poté, co byl agent mostu Connect:Direct vytvořen pomocí příkazu **`fteCreateCDAgent`** , je třeba ručně vytvořit soubor `ConnectDirectCredentials.xml` . Než budete moci používat agenta mostu Connect:Direct , musíte tento soubor upravit, aby zahrnoval informace o hostiteli, uživateli a pověření. Další informace naleznete v tématu Formát souboru pověřeníConnect:Direct. Standardně je tento soubor načtený 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 agent mostu Connect:Direct připojuje. Tato hodnota musí být stejná hodnota, kterou zadáte pro parametr **`fteCreateCDAgent -cdNode`** .

   Hodnota atributu `pattern` může být buď `wildcard` , nebo `regex`. Není-li tento atribut zadán, použije se standardní hodnota `wildcard`.

2. Vložte ID uživatele a informace o pověření do souboru jako podřízené prvky produktu `<tns:pnode>`.

   Do souboru můžete vložit jednu nebo více instancí následujících prvků produktu `<tns:user>` :

```
<tns:user name="name"
          pattern="pattern"
          ignorecase="ignorecase"
          cdUserId="cdUserId"
```

```
          cdPassword="cdPassword"
          pnodeUserId="pnodeUserId"
          pnodePassword="pnodePassword">
</tns:user>
```

kde:

- *name* je vzor, který odpovídá ID uživatele MQMD přidruženému k požadavku na přenos MFT .
- *pattern* uvádí, zda vzor zadaný pro atribut name je výraz se zástupnými znaky, nebo Java regulární výraz. Hodnota atributu pattern může být buď wildcard , nebo regex. Není-li tento atribut zadán, použije se standardní hodnota wildcard.
- Hodnota *ignorecase* určuje, zda má být při zpracování vzorku určeného atributem name rozlišována velká a malá písmena. Není-li tento atribut zadán, použije se standardní hodnota 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 produktu Connect:Direct . Pokud *cdUserId* nemůže být administrátorem serveru Connect:Direct , ujistěte se, že ID uživatele má následující funkční oprávnění na uzlu mostu Connect:Direct :

  – Pro uzel Windows nastavte následující oprávnění. Tento příklad je formátován spolu s návratem vozíku k čitelnosti podpory:

  ```
  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 UNIX nastavte následující parametry v souboru userfile.cfg :

  ```
  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 určenému atributem cdUserId .
- Volitelně můžete zadat atribut pnodeUserId . Hodnota tohoto atributu je ID uživatele, které je používáno uzlem Connect:Direct zadaným atributem name prvku <tns:pnode> k odeslání procesu Connect:Direct . Pokud nezadáte atribut pnodeUserId , bude uzel Connect:Direct používat ID uživatele zadané atributem cdUserId k odeslání procesu Connect:Direct .
- Volitelně můžete zadat atribut pnodePassword. Hodnota tohoto atributu je heslo přidružené k ID uživatele určenému atributem pnodeUserId .

Pokud se žádný prvek uživatele neshoduje s ID uživatele MQMD, přenos selže.

3. Volitelné: Jako podřízené prvky prvku <tns:user> můžete zahrnout jeden nebo více prvků <tns:snode> . Prvek <tns:snode> určuje pověření, která používá uzel 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 produktu Connect:Direct , který je zdrojem nebo cílem přenosu souboru.

   Do souboru vložte jeden nebo více z následujících prvků:

   ```
   <tns:snode name="name"
              pattern="pattern"
              userId="userId"
              password="password"/>
   ```

   kde:

   - *name* je vzor, který se shoduje s názvem uzlu Connect:Direct , který je zdrojem nebo cílem přenosu souboru.
   - *pattern* uvádí, zda vzor zadaný pro atribut name je výraz se zástupnými znaky, nebo Java regulární výraz. Hodnota atributu pattern může být buď wildcard , nebo regex. Není-li tento atribut zadán, použije se standardní hodnota wildcard.
   - *userId* je ID uživatele, které je používáno uzlem Connect:Direct zadaným atributem name prvku <tns:pnode> pro připojení k uzlu Connect:Direct , který odpovídá vzoru určenému atributem name z <tns:snode>.
   - *password* je heslo přidružené k ID uživatele určenému atributem userId .

   Pokud žádný prvek <tns:snode> neodpovídá sekundárnímu uzlu přenosu souboru, nezpůsobí to, že přenos selže. Přenos je spuštěn a nejsou zadány žádné ID uživatele a heslo pro použití v uzlu snode.

Výsledky

Při hledání shody se vzorem pro jména uživatelů nebo názvy uzlů produktu Connect:Direct hledá agent mostu Connect:Direct od začátku souboru na konec souboru. První nalezená shoda je ta, která se používá.

Související úlohy

“Konfigurace mostu produktu Connect:Direct” na stránce 723

Nakonfigurujte most produktu Connect:Direct k přenosu souborů mezi sítí Managed File Transfer a sítí Connect:Direct . Komponenty mostu Connect:Direct jsou uzly produktu Connect:Direct a Managed File Transfer , které jsou vyhrazeny pro komunikaci s tímto uzlem. Na tohoto agenta se odkazuje jako na agenta mostu Connect:Direct .

Související odkazy

Formát souboru pověření Connect:Direct

fteCreateCDAgent: vytvoření agenta mostu Connect:Direct

Mapování pověření pro produkt Connect:Direct pomocí tříd ukončení

Pokud nechcete použít výchozí funkci mapování pověření agenta mostu produktu Connect:Direct , můžete mapovat uživatelská pověření v produktu Managed File Transfer na pověření uživatele na uzlu produktu Connect:Direct zápisem vlastní uživatelské procedury. Konfigurace vašich vlastních uživatelských procedur mapování pověření vypne výchozí funkci mapování pověření.

Informace o této úloze

Uživatelské procedury, které vytvoříte pro mapování Connect:Direct , musí implementovat rozhraní com.ibm.wmqfte.exitroutine.api.ConnectDirectCredentialExit. Další informace viz CDCredentialExit.java interface.

Windows Konfigurace agentů MFT se službou MSCS

Managed File Transfer (MFT) agent Microsoft Cluster Service (MSCS) setup is supported, if the platform is one supported by MFT and running one of the versions of Windows.

Informace o této úloze

Tato úloha popisuje dva scénáře, které můžete sledovat, 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 konfigurovat agenta jako prostředek MSCS, postupujte takto:
  a) Produkt Managed File Transfer nainstalujte lokálně na každý počítač v klastru.

     Viz Instalace produktu 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. Informace o tom, jak to provést, najdete v tématu Nastavení agenta.

  c) Upravte agenta tak, aby se spouštěl jako služba produktu Windows , a nakonfigurujte jej tak, aby se automaticky nespouštěl při restartu produktu Windows nastavením pole **Typ spuštění** pro službu agenta v nástroji služeb Windows na hodnotu `Ruční`.

     Další informace naleznete v tématu Spuštění agenta MFT jako služby systému Windows.

  d) Zopakujte krok “2” na stránce 728 a krok “3” na stránce 728 se scénářem 1 na sekundárním počítači.

     Tím je zajištěno, že struktura souboru 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 728.

  e) Na primárním počítači přidejte agenta jako 'generickou službu' pod ovládací prvek MSCS.

     Postupujte takto:

     a. Klepněte pravým tlačítkem myši na klastr a vyberte volbu **Role-> Přidat prostředek-> 'Generická služba'**.

     b. Ze seznamu služeb produktu 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, pak bude služba agenta spuštěna na jiném počítači.

Scénář 2: Konfigurace správce front agenta a agenta jako prostředků MSCS

- Chcete-li nakonfigurovat správce front agenta a agenta jako prostředky MSCS, proveďte následující kroky:
  a) Konfigurujte správce front agenta tak, aby se spouštěl jako prostředek MSCS.

     Informace o tom, jak to provést, viz “Vložení správce front do ovládacího prvku MSCS” na stránce 446.

  b) Vytvořte agenta na primárním počítači v klastru.

     Agent by měl být konfigurován tak, aby se připojil ke správci front agenta pomocí přenosu BINDINGS. Ujistěte se, že jste vytvořili všechny objekty ve správci front pro tohoto agenta. Informace o tom, jak to provést, najdete v tématu Nastavení agenta.

  c) Upravte agenta tak, aby se spouštěl jako služba produktu Windows , a nakonfigurujte jej tak, aby se automaticky nespouštěl při restartu produktu Windows nastavením pole **Typ spuštění** pro službu agenta v nástroji služeb Windows na hodnotu `Ruční`.

Další informace naleznete v tématu Spuštění agenta MFT jako služby systému Windows.

d) Ujistěte se, že je na sekundárním počítači spuštěn správce front agenta (který je pod řízením MSCS).

   Agent vytvořený na tomto počítači se připojí ke správci front pomocí přenosu BINDINGS, a proto musí být k dispozici při vytvoření agenta.

e) Zopakujte krok “2” na stránce 728 a krok “3” na stránce 728 se scénářem 2 na sekundárním počítači.

   Tím je zajištěno, že struktura souboru 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 728.

f) Přidejte agenta jako 'generickou službu' pod řídicí prvek MSCS.

   Postupujte takto:

   a. Klepněte pravým tlačítkem myši na klastr a vyberte volbu **Role-> Přidat prostředek-> 'Generická služba'**.

   b. Ze seznamu služeb produktu Windows vyberte službu agenta a dokončete průvodce konfigurací klepnutím na tlačítko **Další**.

g) Upravte vlastnosti prostředku služby agenta tak, aby bylo možné přidat prostředek správce front do seznamu závislostí.

   To zajistí, aby byl prostředek správce front spuštěn dříve, než bude agent spuštěn.

h) Převeďte prostředek správce front do režimu offline a poté přeneste prostředek agenta do režimu online. Ověřte, zda je spuštěn jak prostředek správce front, tak i agent.

   Pokud dojde k překonání selhání, pak se na sekundárním počítači spustí služba agenta a správce front agenta.

V 9.1.4 Vysoce dostupné agenty v produktu Managed File Transfer

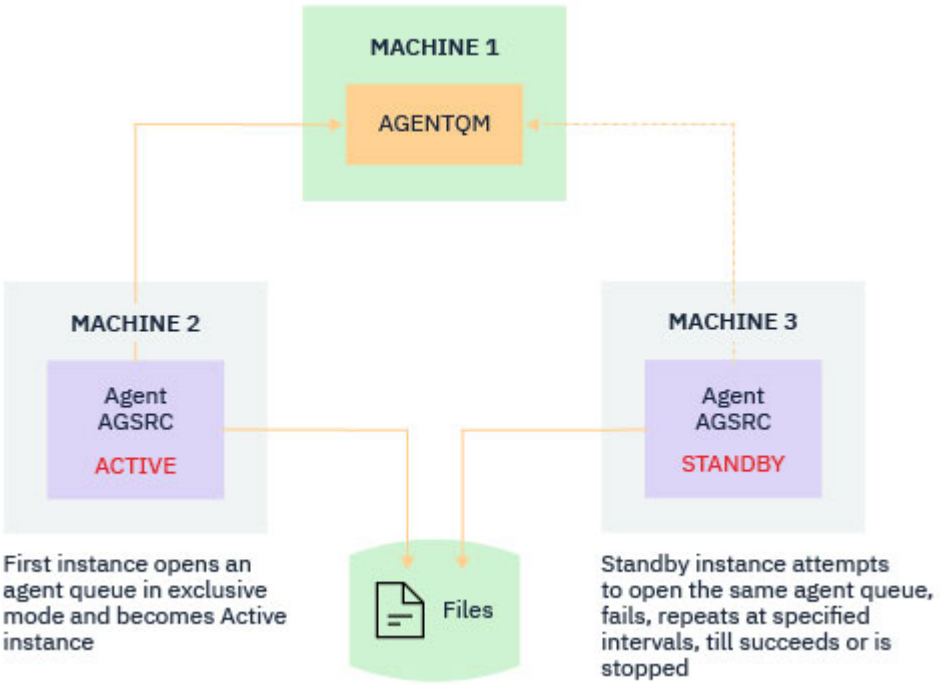
V produktu IBM MQ 9.1.4můžete nakonfigurovat standardní agenty nebo agenty mostu v produktu MFT tak, aby byly spouštěny v konfiguraci vysoké dostupnosti (HA). Dvojice instancí agenta s identickými konfiguracemi je zahrnuta do nastavení vysoké dostupnosti, kdy jedna instance běží na jednom počítači, zatímco jiná instance je spuštěna na jiném počítači. Obě instance jsou nakonfigurovány pro připojení ke stejnému správci front agenta.

Přehled

Pouze jedna, nazývaná *aktivní instance*dvou instancí, zpracovává přenosy souborů, zatímco druhá instance, která se nazývá *rezervní instance*, je ve stavu, kdy může dokončit svou inicializaci a převzít přenosy souborů, ale nezpracovává žádné přenosy souborů.

Když aktivní instance selže nebo ztratí připojitelnost ke správci front, rezervní instance dokončí svou inicializaci, stane se aktivní a zahájí zpracování přenosů souborů. Všechny přenosy inflight, které probíhaly, když se aktivní instance obnovily z posledního známého kontrolního bodu.

Následující ilustrace zobrazuje společnou konfiguraci aktivních a rezervních



agentů:

Notes:

1. Jedna instance agenta je spuštěna na dvou různých počítačích, s jednou z instancí jako aktivní instance a druhou jako instance v pohotovostním režimu.
2. Přenosy do aktivních instancí procesů jsou pouze aktivní. Rezervní instance se nachází v nečinném stavu, čeká se na přechod aktivní instance na nižší úroveň.
3. Stejná sada front agenta je sdílena mezi dvěma instancemi agenta.
4. Obě instance agenta potřebují přístup ke stejnému sdílenému systému souborů, aby mohly provádět spravované přenosy.

Aktivní mechanizmus instance agenta v aktivním pohotovostním režimu pracuje tak, že se uzamkne sdíleného prostředku, jako například správci front IBM MQ s více instancemi. Instance agenta, která převezme zámek na sdíleném prostředku, se stane aktivní instancí, zatímco druhá instance (která selže při převzetí zámku) se stane rezervní instancí.

Sdílený prostředek je zde nová fronta, SYSTEM.FTE.HA.<agent name>. Tato fronta se vytvoří automaticky, když je konfigurován agent IBM MQ 9.1.4 .

Jak proces pracuje

Chcete-li vytvořit agenta HA, vytvořte agenta se shodnými konfiguračními parametry na dvou počítačích spuštěním příkazu **fteCreateAgent** nebo **fteCreateBridgeAgent** s použitím přídavného parametru **-x** společně s vlastností agenta **highlyAvailable** v souboru agent.properties nastaveným na hodnotu true.

Notes:

- Obě konfigurace musí ukazovat na stejného správce front agenta.
- Požadované fronty agentů se musí vytvořit pouze jednou ve správci front agenta.

Další informace o parametru **-x** a o souboru agent.properties naleznete v popisu příkazu **fteCreateAgent** a další informace o vlastnosti agenta **highlyAvailable** .

Všimněte si, že spuštění příkazu vytvoří soubor MQSC obsahující skripty, které jsou nezbytné k vytvoření objektů IBM MQ ve správci front agenta a ve frontě <SYSTEM.FTE.HA.*agent name* bez ohledu na to, zda jste zadali parametr **-x** nebo ne.

Při vytváření vysoce dostupné konfigurace agenta příkaz **fteCreateAgent** nebo **fteCreateBridgeAgent** kontroluje existenci instance stejného agenta přítomného na jiném místě přihlášením k odběru tématu SYSTEM.FTE/Agents/*agent name* . Je-li nalezena instance stejného agenta, pak buď příkaz vytvoří požadovanou konfiguraci na systému souborů, ale nepublikuje vytvoření agenta znovu.

Když se agent spustí v režimu HA:

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 z ní *aktivní instance* agenta a další proces spuštění pokračuje.
3. Pokud pokus o otevření fronty SYSTEM.FTE.HA.*agent name* ve výlučném režimu GET selže s kódem příčiny MQRC_OBJECT_IN_USE, znamená to, že již existuje aktivní instance agenta, který je spuštěn jinde. Proto se tato instance stane *záložní instancí* agenta.

   Rezervní instance se pokusí otevřít frontu SYSTEM.FTE.HA.<agent name> v určených intervalech. Pro tento účel je v souboru agent.properties poskytována další vlastnost agenta **standbyPollInterval** .

   Při použití výchozí hodnoty se záložní instance pokusí otevřít frontu SYSTEM.FTE.HA.*agent name* každých pět sekund. Opakuje se, dokud se instance nepodaří otevřít frontu SYSTEM.FTE.HA.*agent name* nebo se zastaví pomocí příkazu **fteStopAgent** .

Více rezervních instancí

Všechny instance v pohotovostním režimu 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 instancích v pohotovostním režimu a publikuje informace jako část publikace stavu agenta. V produktu IBM MQ 9.1.4se výstup příkazu **fteShowAgentDetails** , odezva agenta GET REST API a modul plug-in IBM MQ Explorer MFT zobrazí informace o všech rezervních instancích.

Další informace viz příklady výstupů příkazu **fteShowAgentDetails** a odpovědi agenta GET REST API .

Příklady informací o stavu agenta ve formátu XML viz Stavové zprávy agentaMFT .

Požadavek na verzi

Aktivní a záložní agenti musí být IBM MQ 9.1.4 nebo vyšší.

Upozornění:

- Verze produktu IBM MQ před verzí IBM MQ 9.1.4 nelze konfigurovat nebo spustit v režimu s vysokou dostupností.
- Aktivní i rezervní instance musí spouštět stejnou verzi kódu.

Verze aktivní a rezervní instance se validuje, aby se zajistilo, že obě instance mají stejnou verzi.
Pro komunikaci mezi instancemi se používá dočasná dynamická fronta. Dva vlastnosti agenta, **dynamicQueuePrefix** a **modelQueueName**, definované v souboru agent.properties , vygenerují název dočasné dynamické fronty.

V 9.1.4 Požadované informace pro vysoce dostupné agenty v produktu Managed File Transfer

Existují různé typy informací, které potřebujete znát o standardních agentech nebo agentech MFT , kteří jsou spuštění 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 režimu vysoké dostupnosti

Pokud je proveden pokus o spuštění další instance agenta, která není konfigurována jako agent vysoké dostupnosti, je nejprve provedena kontrola, zda lze zámek získat ve frontě SYSTEM.FTE.HA.*agent name* .

Vzhledem k tomu, že byla spuštěna jiná instance v jiném než režimu vysoké dostupnosti, bude touto instancí získán zámek ve frontě produktu SYSTEM.FTE.HA.*agent name* . Agent pokračuje v inicializaci, ale později selže, protože je fronta příkazů otevřena exkluzivně pro jinou instanci.

V tomto případě se zprávy zobrazené v následujícím příkladu zaprotokolují do souboru output0.log agenta a agent pokračuje ve svém pokusu otevřít frontu příkazů každých 30 sekund:

```
BFGMQ1045I: Systémová fronta agenta 'SYSTEM.FTE.COMMAND.SRC' je konfigurován buď jako NOSHARE,
nebo
DEFSOPT (SDÍLENÝ).

BFGAG0035W: Agent obdržel při pokusu o otevření fronty kód příčiny MQI 2042.
'SYSTEM.FTE.COMMAND.SRC'na správci front' MFTHAQM 's názvem připojení' localhost (1414) '
a kanál 'MFT_HA_CHN'.  Agent se pokusí o operaci znovu každých 30 sekund.
```

Instance agenta je spuštěna v režimu vysoké dostupnosti jinde

Pokud je proveden pokus o spuštění další instance agenta, která není konfigurována jako agent vysoké dostupnosti, je nejprve provedena kontrola, zda lze zámek získat ve frontě SYSTEM.FTE.HA.*agent name* .

Protože druhá instance byla spuštěna jako aktivní instance, pokus o získání zámku selže. Spuštění instance se nezdaří a následující chybová zpráva se zaprotokoluje do souboru output0.log agenta:

```
BFGAG0194E: Instance tohoto agenta je již spuštěna jinde.
Proto tato instance nemůže pokračovat, a bude ukončena.
```

Windows Spuštění agenta jako služby Windows

V systému Windowsmůžete spustit agenta jako službu Windows .

Při spuštění produkt Windows spustí agenta MFT v normálním režimu nebo v režimu HA. Je-li agent konfigurován 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 označovaly typ instance. Když se instance agenta spustí jako aktivní instance, zapíše se následující zpráva:

```
BFGAG0193I: Agent byl úspěšně inicializován jako aktivní instance.
```

Když se instance agenta spustí jako instance v pohotovostním režimu, zapíše se následující zpráva:

```
BFGAG0193I: Agent byl úspěšně inicializován jako instance v pohotovostním režimu.
```

Aktualizace stavu agenta

Jelikož 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 instancí v pohotovostním režimu.

Pro tento účel jsou v souboru agent.properties k dispozici dvě další vlastnosti:

- **standbyStatusExpiry** je doba vypršení platnosti stavové zprávy o stavu pohotovosti, která se má umístit do fronty příkazů agenta. Zpráva vyprší, pokud aktivní instance agenta tuto zprávu v daném období nezpracuje.

  Ve výchozím nastavení je hodnota **standbyStatusExipry** 30 sekund. Zpráva je také nízká priorita, 9, zpráva pro umožnění zpracování priority požadavků na přenos přes stavové zprávy v pohotovostním režimu.
- **standbyStatusPublishInterval** nastavuje frekvenci, s jakou rezervní instance publikuje svůj stav.

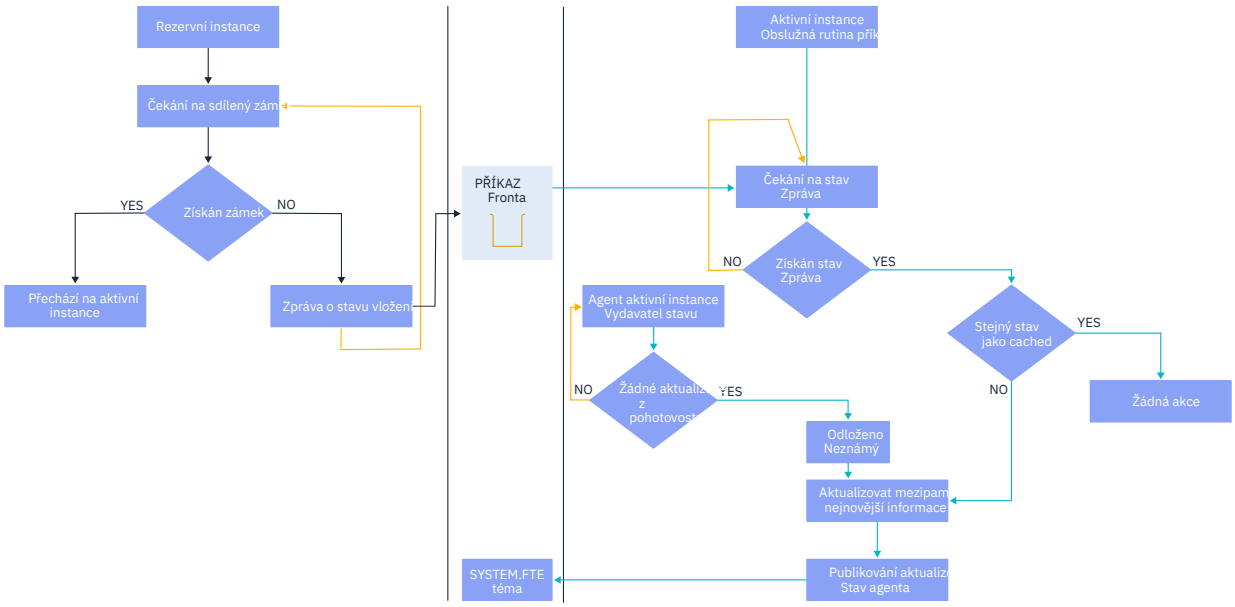
Aktivní instance

Aktivní instance provádí zpracování aktualizací stavu z instance v pohotovostním režimu:

1. Získá zprávu z fronty SYSTEM.FTE.COMMAND.<agent name> a deleguje zpracování zpráv na pracovní podproces.
2. Pracovní podproces načte obsah z těla zprávy, aktualizuje objekt stavu agenta s informacemi o instanci v pohotovostním režimu a oznámí vydavateli stavu agenta, aby publikoval stav.
3. Vydavatel stavu agenta publikuje stav.

   Všimněte si, že optimalizace se zde provádějí k ukládání informací o stavu pohotovosti do mezipaměti. Když je učiněn požadavek, vydavatel stavu agenta zkontroluje nový stav se stavem uloženým v mezipaměti a publikuje se pouze, pokud existuje rozdíl.

Následující diagram popisuje tok aktivních nebo záložních instancí za účelem publikování stavu agenta:



V 9.1.4 Vyřazení instancí, překonání selhání a údržby ve vysoce dostupných agentech

Vysoce dostupné instance produktu Managed File Transfer lze vyřadit, lze je různými způsoby selhovat a mohou vyžadovat údržbu.

Vyřazení stavu instance v pohotovostním režimu

Mohou existovat situace, kdy je aktivní instance zaneprázdněna přenosy a není schopna zpracovat stavové zprávy instance v pohotovostním režimu, nebo se záložní instance nezdařila, nebo z jakéhokoli důvodu nezveřejňuje stavové zprávy.

V takových situacích aktivní agent, který byl informován o přítomnosti instance v pohotovostním režimu, čeká na hodnotu zadanou vlastností **standbyStatusDiscardTime** v souboru agent.properties

před odebráním záložní instance ze seznamu. Výchozí hodnota této vlastnosti je 600 sekund, což je dvojnásobek hodnoty vlastnosti **standbyStatusPublishInterval** .

Selhání instance normálně

Chcete-li provést normální překonání selhání, musíte použít příkaz **fteStopAgent** s volbou **-i** .

Tím je zajištěno, že je aktivní instance okamžitě zastavena. Pokud zastavíte agenta bez volby **-i** , agent bude pokračovat ve zpracování, dokud nebudou všechny probíhající přenosy dokončeny aktivní instancí, a proto může překonání selhání trvat dlouho.

Všechny přenosy inflight transfers se obnoví od posledního známého kontrolního bodu.

Selhávání v instanci v jiných situacích

Pokud je aktivní instance ukončena způsobem, který není normální, nebo dojde k selhání celého počítače, připojení ke frontě agenta je přerušeno a správce front zavře všechny otevřené fronty včetně fronty SYSTEM.FTE.HA.<agent name> a připojení.

V důsledku toho získá rezervní instance výlučnou operaci GET a dokončí zbytek inicializace agenta.

Opět platí, že všechny inflight transfers resume from the last known check points.

Pokud se připojení ke správci front přeruší

Režim klienta

Proces agenta se skládá z několika podprocesů. Jiný než výchozí podprocesy, například podproces, který publikuje stav agenta v pravidelných intervalech, je každý požadavek na přenos zpracován se sadou podprocesů, které končí po dokončení přenosu.

Mnohé z těchto podprocesů se připojují ke správci front agenta a zobrazují a získují zprávy. Je možné, že některé z těchto připojení mohou být přerušeními kvůli problémům se sítí nebo selháním správce front. Pokud některý podproces zjistí problém s porušeným připojením, informuje o zahájení zotavení podproces hlavní podproces a ukončí jej.

Hlavní podproces poté spustí další podproces, aby počkal na navázání připojení ke správci front. Jakmile se znovu připojíte, provede se pokus o získání výlučného GET pro agenta. Je-li toto úspěšné, agent pokračuje v dokončení obnovy a stane se aktivní instancí. Pokud se pokus o získání výhradního GET nezdaří, instance se stane rezervní.

Režim vazeb

Při připojování v režimu vázání, pokud agent ztratí připojení, proces agenta skončí. Řadič procesů obslouží restartování agenta. Když se agent restartuje, prochází procesem pokusu o získání výlučného GET pro sebe.

Pokud agent uspěje, stane se z aktivní instance; jinak se agent stane rezervní instancí.

Použití aktualizací úrovně údržby

Kroky pro použití údržby na vysoce dostupné agenty jsou podobné těm, které jsou dokumentovány pro správce front s více instancemi. Další informace naleznete v tématu Použití aktualizací úrovně údržby na správce front pro více instancí v produktu Windows, Použití aktualizací úrovně údržby na správce front pro více instancí v produktu AIX, Použití aktualizací úrovně údržby pro správce front s více instancemi v produktu Solaris nebo Použití aktualizací úrovně údržby na správce front s více instancemi v produktu Linux.

Než použijete údržbu, musíte zastavit agenta spuštěného na počítači, na kterém se má použít úroveň údržby. Pokud aktualizujete aktivní instanci, kvůli kontinuitě přenosů, musíte provést překonání selhání aktivní instance na instanci v pohotovostním režimu.

Jakmile je upgrade dokončen, musíte spustit instanci agenta, překonání selhání aktuální aktivní instance na upgradovanou instanci a poté upgradovat instanci v pohotovostním režimu.

Migrace agentů ze starší verze produktu

Agenti migrované z verzí produktu IBM MQ před spuštěním produktu IBM MQ 9.1.4 jsou spuštění jako nevysoce dostupné. Můžete je spustit v režimu vysoké dostupnosti podle postupu v tématu Migrace agentů Managed File Transfer z dřívější verze.

V 9.1.0 Konfigurace produktů IBM MQ Console a REST API

Server mqweb, který je hostitelem produktů IBM MQ Console a REST API , je dodáván spolu s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh, jako je například konfigurace zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny volby konfigurace, které jsou k dispozici.

Procedura

- "Konfigurace zabezpečení" na stránce 739
- "Konfigurace názvu hostitele HTTP" na stránce 739
- "Konfigurace portů HTTP a HTTPS" na stránce 740
- "Konfigurace časového limitu odezvy" na stránce 741
- "Konfigurace automatického spuštění" na stránce 742
- "Konfigurace protokolování" na stránce 743
- "Konfigurace tokenu LTPA" na stránce 745
- "Konfigurace brány administrative REST API" na stránce 747
- "Konfigurace messaging REST API" na stránce 748
- "Konfigurace produktu REST API for MFT" na stránce 750
- "Vyladění prostředí JVM serveru mqweb" na stránce 752
- "Struktura souborů instalační komponenty produktů IBM MQ Console a REST API" na stránce 753
- "Konfigurace záznamu použití webového serveru mqweb v systému z/OS" na stránce 755

Základní konfigurace pro server mqweb

Než budete moci začít používat produkt REST API nebo IBM MQ Console, musíte nainstalovat správné komponenty a nakonfigurovat server mqweb, který je hostitelem produktu REST API nebo produktu IBM MQ Console.

Informace o této úloze

Procedura pro tuto úlohu se zaměřuje na základní konfiguraci pro server mqweb, abyste mohli rychle začít pracovat s produkty REST API a IBM MQ Console. Kroky pro konfiguraci zásady zabezpečení popisují, jak nastavit základní registr uživatelů, ale existují další volby pro konfiguraci uživatelů a rolí. Další informace o konfiguraci zabezpečení pro protokol mqweb naleznete v příručce IBM MQ Console and REST API security.

Poznámka: Chcete-li dokončit tento postup, musíte mít přístup k souboru `mqwebuser.xml` :

- z/OS V systému z/OSmusíte být uživatel, který má přístup pro zápis k souboru `mqwebuser.xml` .
- Multi Na všech ostatních operačních systémech musíte být privilegovaný uživatel , abyste měli přístup k souboru `mqwebuser.xml` .

Postup

1. Nainstalujte komponentu IBM MQ Console a REST API :
   - AIX V systému AIXnainstalujte sadu souborů `mqm.web.rte` . Další informace o instalaci sad souborů v systému AIXnaleznete v tématu Úlohy instalace produktuAIX.
   - IBM i V systému IBM inainstalujte webovou komponentu. Chcete-li tuto funkci použít, musíte také nainstalovat prostředí Java Messaging a webové služby produktu 5724L26 IBM MQ a předpoklady pro prostředí Java SE 8 produktu 5770JV1 . Další informace o instalaci funkcí v systému IBM inaleznete v tématu Úlohy instalace produktuIBM i.
   - Linux V systému Linuxnainstalujte komponentu produktu `MQSeriesWeb` . Další informace o instalaci komponent v systému Linuxnaleznete v tématu Úlohy instalace produktuLinux.
   - Solaris V systému Solarisnainstalujte komponentu produktu `web` . Další informace o instalaci komponent v systému Solarisnaleznete v tématu Úlohy instalace produktuSolaris.
   - Windows V systému Windowsnainstalujte funkci `Web Administration` . Další informace o instalaci funkcí v systému Windowsnaleznete v tématu Úlohy instalace produktuWindows.
   - z/OS V systému z/OSnainstalujte funkci `IBM MQ for z/OS Unix System Services Web Components` . Další informace o instalaci komponent a funkcí v systému z/OSnaleznete v tématu Úlohy instalace produktuz/OS.
2. z/OS
   V systému z/OSvytvořte mqweb server, který je hostitelem produktů IBM MQ Console a REST API spuštěním skriptu **crtmqweb** .

   Tento skript vytvoří adresář uživatelů produktu WebSphere Liberty , který obsahuje konfiguraci a soubory protokolu mqweb serveru. Další informace o spuštění skriptu **crtmqweb** viz “Vytvoření serveru mqweb” na stránce 860.
3. z/OS
   V systému z/OSvytvořte katalogovou proceduru pro spuštění serveru mqweb.

   Další informace viz téma “Vytvoření procedury pro mqweb server” na stránce 862.
4. Nahraďte existující konfigurační soubor `mqwebuser.xml` se základním souborem ukázek registru, který je nakonfigurován tak, aby nabízel základní zabezpečení. Zkopírujte soubor `basic_registry.xml` z adresáře *MQ_INSTALLATION_PATH*`/web/mq/samp/configuration` do odpovídajícího adresáře pro váš systém a přejmenujte jej na `mqwebuser.xml`:
   - Linux UNIX V systémech UNIX a 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 produktu IBM MQ , tato cesta je datová cesta, která je vybrána během instalace produktu IBM MQ. Při výchozím nastavení 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** za účelem vytvoření definice mqweb serveru.

   Ukázkový soubor `basic_registry.xml` konfiguruje čtyři uživatele:

   MQADMIN
   Administrativní uživatel, který je členem role MQWebAdmin .

   mqreader
   Administrativní uživatel s oprávněním jen pro čtení, který je členem role MQWebAdminRO.

mftadmin
Administrativní uživatel, který je členem role MFTWebAdmin .

mftreader
Administrativní uživatel s oprávněním jen pro čtení, který je členem role MFTWebAdminRO.

Všichni uživatelé jsou také členy role MQWebUser .

Další informace o dostupných rolích najdete v tématu Role na serveru IBM MQ Console a REST API

5. Volitelné: Upravte soubor `mqwebuser.xml` a přidejte další uživatele a skupiny. Přiřaďte tyto uživatele a seskupte odpovídající role, abyste byli autorizováni používat produkt REST API nebo IBM MQ Console. Můžete také změnit hesla pro uživatele, kteří jsou nadefinovali při výchozím nastavení, a zakódovat nová hesla. Další informace viz téma Konfigurace uživatelů a rolí.

   Poznámka:

   - z/OS Pokud v produktu z/OSpřidáte uživatele do role MQWebUser , musíte také udělit alternativní uživatelský přístup pro alternativní ID uživatele mqweb 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 ve vašem systému stejný název jako existující uživatel produktu IBM MQ . Po stejném formátu jako ostatní uživatelé v souboru xml přidejte ID uživatele a heslo za následující řádek v souboru xml: `<user name="mftreader" password="mftreader"/>`.

6. z/OS
   V systému z/OSnastavte proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci vašeho mqweb serveru, zadáním následujícího příkazu:

   ```
   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” na stránce 860.

7. Ve výchozím nastavení jsou produkty REST API a IBM MQ Console dostupné pouze ze stejného hostitele jako je mqweb server. Zadáním následujícího příkazu povolte vzdálená připojení k mqweb serveru:

   ```
   setmqweb properties -k httpHost -v hostname
   ```

   Kde parametr *název_hostitele* určuje adresu IP, název hostitele DNS (Domain Name Server) s příponou názvu domény nebo název hostitele DNS pro server, na kterém je nainstalován produkt IBM MQ . Chcete-li určit všechna dostupná síťová rozhraní, použijte hvězdičku (*), jak je uvedeno v následujícím příkladu:

   ```
   setmqweb properties -k httpHost -v "*"
   ```

8. Volitelné: Ve výchozím nastavení není volba administrative REST API pro MFT povolena. Chcete-li tuto funkci použít, musíte ji povolit a nakonfigurovat správce koordinační fronty:

   a) Povolte administrative REST API for MFT zadáním následujícího příkazu:

   ```
   setmqweb properties -k mqRestMftEnabled -v true
   ```

   b) Zadáním následujícího příkazu konfigurujte správce front, který je správcem front koordinace:

   ```
   setmqweb properties -k mqRestMftCoordinationQmgr -v qmgrName
   ```

Kde *qmgrName* je název koordinačního správce front.

c) CD

Chcete-li povolit volání testu 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.

Poznámka: Tento krok platí od verze IBM MQ 9.1.2.

9. Spusťte mqweb server, který podporuje REST API a IBM MQ Console:

- ULW V systému UNIX, Linux, and Windowszadejte jako privilegovaný uživatelnásledující příkaz:

```
strmqweb
```

- IBM i V systému IBM ijako privilegovaný uživatelzadejte do prostředí Qshell následující příkaz:

```
/QIBM/ProdData/mqm/bin/strmqweb
```

- z/OS V systému z/OSspusťte proceduru, kterou jste vytvořili v produktu “Vytvoření procedury pro mqweb server” na stránce 862.

  Následující zprávy jsou vydány do STDOUT DD, aby se označilo, že byl úspěšně spuštěn mqweb server.

```
[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 mqweb na serveruz/OSnebo pomocí příkazu **endmqweb** . Pokud však není spuštěn server mqweb, nelze použít REST API ani IBM MQ Console.

10. z/OS

Volitelné: Chcete-li v produktu z/OSpovolit, aby produkty pro automatizaci systému zachycly zprávy MQWB2019I a MQWB0023I , které jsou vydány při spuštění produktu MQ Console a produktu REST API , nakonfigurujte server mqweb tak, aby tyto zprávy zapisoval do konzoly produktu MVS . Chcete-li nakonfigurovat server mqWeb pro zápis zpráv MQWB2019I a MQWB0023I do konzoly produktu MVS , upravte soubor `mqwebuser.xml` , který jste vytvořili v kroku “4” na stránce 736, a přidejte do souboru následující řádek:

```
<zosLogging enableLogToMVS="true" wtoMessage="MQWB2019I,MQWB0023I"/>
```

Další informace o konfiguraci protokolování produktu z/OS na webovém serveru mqweb naleznete v tématu Protokolování produktuz/OS (zosLogging).

Jak pokračovat dále

1. Konfigurujte nastavení serveru mqweb, včetně povolení připojení HTTP, a změna čísla portu. Další informace viz téma “Konfigurace produktů IBM MQ Console a REST API” na stránce 735.
2. Volitelně nakonfigurujte REST API:

   a. Nakonfigurujte sdílení prostředků různého původu pro REST API. Standardně nemůžete přistoupit k produktu REST API z webových prostředků, které nejsou hostovány na stejné doméně jako REST API. To znamená, že požadavky typu cross-origin nejsou povoleny. Sdílení CORS (Cross Origin

Resource Sharing) můžete nakonfigurovat tak, aby bylo možné povolit požadavky na křížový původ ze zadaných adres URL. Další informace naleznete v tématu Konfigurace CORS pro produkt REST API.

b. Nakonfigurujte REST API pro MFT. Další informace viz téma “Konfigurace produktu REST API for MFT” na stránce 750.

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 9.1.0 Konfigurace zabezpečení

Zabezpečení pro IBM MQ Console a REST API můžete nakonfigurovat úpravou souboru `mqwebuser.xml` . Uživatele můžete nakonfigurovat a ověřit tak, že nakonfigurujete buď základní registr uživatelů, nebo registr LDAP, nebo jakýkoli jiný typ registru, který se dodává s produktem WebSphere Liberty. Tyto uživatele pak můžete autorizovat přiřazením uživatelů a skupin k roli.

Informace o této úloze

Chcete-li konfigurovat zabezpečení pro IBM MQ Console, a REST API, musíte konfigurovat uživatele a skupiny. Tito uživatelé a skupiny pak mohou být autorizováni používat IBM MQ Console, nebo REST API, nebo obojí. Další informace o konfiguraci uživatelů a skupin a ověřování a ověřování uživatelů naleznete v tématu Zabezpečení produktuIBM MQ a REST API.

Když se uživatelé ověřují pomocí produktu IBM MQ Console, vygeneruje se token LTPA. Tento token umožňuje uživateli používat produkt IBM MQ Console bez opětovného ověření, dokud nevyprší platnost tokenu.

Pokud používáte ověření založené na tokenech se serverem REST API, vygeneruje se při přihlášení uživatele pomocí prostředku `/login` REST API s metodou HTTP POST jiný token LTPA. Můžete nakonfigurovat, kdy tento token vyprší, a zda lze tento token použít pro připojení HTTP i HTTPS. Další informace viz “Konfigurace tokenu LTPA” na stránce 745.

Procedura

- zabezpečení produktuIBM MQ Console a REST API
- “Konfigurace tokenu LTPA” na stránce 745

V 9.1.0 Konfigurace názvu hostitele HTTP

Ve výchozím nastavení je server mqweb, který je hostitelem produktů IBM MQ Console a REST API , konfigurován tak, aby povoloval pouze lokální připojení. To znamená, že IBM MQ Console a REST API jsou přístupné pouze na systému, na kterém jsou nainstalovány produkty IBM MQ Console a REST API . Chcete-li povolit vzdálená připojení pomocí příkazu **setmqweb** , můžete nakonfigurovat název hostitele.

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/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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 názvu hostitele HTTP pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole httpHost zobrazuje název hostitele HTTP. Další informace viz dspmqweb.
- Nastavte název hostitele HTTP pomocí následujícího příkazu:

  ```
  setmqweb properties -k httpHost -v hostName
  ```

  kde parametr *hostName* určuje adresu IP, název hostitele DNS (Domain Name Server) s příponou názvu domény nebo název hostitele DNS pro server, na kterém je nainstalován produkt IBM MQ . Chcete-li zadat všechna dostupná síťová rozhraní, použijte hvězdičku v uvozovkách. Použijte hodnotu localhost k povolení pouze lokálních připojení.
- Zrušte nastavení názvu hostitele HTTP pomocí následujícího příkazu:

  ```
  setmqweb properties -k httpHost -d
  ```

V 9.1.0 Konfigurace portů HTTP a HTTPS

Ve výchozím nastavení používá server mqweb, který je hostitelem produktů IBM MQ Console a REST API , port HTTPS 9443. Port, který je přidružen k připojení HTTP, je vypnutý. Můžete povolit port HTTP, nakonfigurovat jiný port HTTPS, nebo zakázat port HTTP nebo HTTPS. Porty můžete konfigurovat pomocí příkazu **setmqweb** .

Než začnete

Pokud povolíte port HTTP a používáte ověřování založené na tokenech, musíte povolit stejný token LTPA, který bude použit pro připojení HTTP i HTTPS. Další informace viz téma “Konfigurace tokenu LTPA” na stránce 745.

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru mqwebuser.xml .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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

- Prohlédněte si aktuální konfiguraci portů HTTP a HTTPS pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `httpPort` zobrazuje port HTTP a v poli `httpsPort` je uveden port HTTPS. Další informace viz dspmqweb.
- Povolte nebo nakonfigurujte port HTTP: Použijte tento příkaz:
  - 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 tak, že použijete hodnotu `-1`.
  - Resetujte hodnotu portu HTTP na výchozí hodnotu `-1` pomocí následujícího příkazu:

    ```
    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 tak, že použijete hodnotu `-1`.
  - Resetujte číslo portu HTTPS na standardní hodnotu 9443 pomocí následujícího příkazu:

    ```
    setmqweb properties -k httpsPort -d
    ```

V 9.1.0 Konfigurace časového limitu odezvy

Je-li doba potřebná k odeslání odpovědi zpět klientovi delší než 30 sekund, standardně IBM MQ Console a REST API vyprší časový limit. IBM MQ Console a REST API můžete nakonfigurovat 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/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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

- Pomocí následujícího příkazu zobrazte aktuální konfiguraci časového limitu požadavku:

  ```
  dspmqweb properties -a
  ```

  Pole mqRestRequestTimeout zobrazuje aktuální hodnotu pro časový limit odezvy. Další informace viz dspmqweb.
- Nastavte časový limit požadavku pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestRequestTimeout -v timeout
  ```

  kde parametr *časový limit* určuje časový interval v sekundách před vypršením časového limitu.
- Nastavte časový limit požadavku na výchozí hodnotu 30 sekund pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestRequestTimeout -d
  ```

V 9.1.0 Konfigurace automatického spuštění

Ve výchozím nastavení je při spuštění příkazu mqweb automaticky spuštěn příkaz IBM MQ Console . Můžete nakonfigurovat, zda se IBM MQ Console a REST API spustí automaticky 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/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru mqwebuser.xml .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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 automatického spuštění pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole mqRestAutostart zobrazuje, zda je REST API automaticky spuštěno, a pole mqConsoleAutostart zobrazuje, zda je IBM MQ Console automaticky spuštěn. Další informace viz dspmqweb.

- Konfigurujte, zda se produkt 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.
- Konfigurujte, zda se produkt 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.

V 9.1.0 Konfigurace protokolování

Můžete konfigurovat úrovně protokolování, maximální velikost souboru protokolu a maximální počet souborů protokolu používaných serverem mqweb, který je hostitelem produktů IBM MQ Console a REST API. Protokolování je možné 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/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Informace o této úloze

Soubory protokolu pro mqweb server lze nalézt v jednom z následujících adresářů:

- ULW V systému UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb/logs`
- z/OS V systému z/OS: *WLP_user_directory*`/servers/mqweb/logs`

  kde *WLP_user_directory* je adresář, který byl zadán při spuštění skriptu V 9.1.0 **crtmqweb** za účelem vytvoření definice mqweb serveru.

Trasovací soubory systému zpráv pro server mqweb lze najít v jednom z následujících adresářů:

- ULW V systému UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
- z/OS V systému z/OS: *WLP_user_directory*`/servers/mqweb`

  kde *WLP_user_directory* je adresář, který byl zadán při spuštění skriptu V 9.1.0 **crtmqweb** za účelem vytvoření definice mqweb serveru.

Další informace o povolení trasování pro IBM MQ Console a REST APInajdete v tématu Trasování IBM MQ Console a REST API.

Procedura

- Prohlédněte si aktuální konfiguraci protokolování produktu REST API pomocí následujícího příkazu:

  `dspmqweb properties -a`

  Pole `maxTraceFileSize` zobrazuje maximální velikost souboru trasování, pole `maxTraceFiles` zobrazuje maximální počet trasovacích souborů a pole `traceSpec` zobrazuje úroveň použitého trasování. Kromě toho pole `maxMsgTraceFileSize` zobrazuje maximální velikost souboru trasování

systému zpráv a v poli `maxMsgTraceFiles` je uveden maximální počet souborů trasování systému zpráv. Další informace viz dspmqweb.

- Konfigurujte maximální velikost souboru protokolu:
  - Nastavte maximální velikost souboru protokolu pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxTraceFileSize -v size
    ```

    kde parametr *velikost* určuje velikost (v MB), kterou může každý soubor protokolu dosáhnout pro IBM MQ Console.
  - Pomocí následujícího příkazu resetujte maximální velikost souboru protokolu na výchozí hodnotu 20 MB:

    ```
    setmqweb properties -k maxTraceFileSize -d
    ```
- Nakonfigurujte maximální počet souborů, které se mají použít pro protokolování:
  - Nastavte maximální počet souborů, které se mají použít pro protokolování, pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxTraceFiles -v max
    ```

    kde *max* uvádí maximální počet souborů pro IBM MQ Console.
  - Pomocí následujícího příkazu resetujte maximální počet souborů, které se mají použít pro protokolování, na výchozí hodnotu 2:

    ```
    setmqweb properties -k maxTraceFiles -d
    ```
- Konfigurujte maximální velikost trasování systému zpráv:
  - Nastavte maximální velikost trasování zpráv pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxMsgTraceFileSize -v size
    ```

    kde parametr *velikost* určuje velikost (v MB), kterou může každý soubor protokolu dosáhnout.
  - Nastavte maximální velikost souboru protokolu na výchozí hodnotu 200 MB pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxMsgTraceFileSize -d
    ```
- Nakonfigurujte maximální počet souborů trasování systému zpráv, které mají být použity:
  - Nastavte maximální počet souborů, které mají být použity pro trasování systému zpráv, pomocí následujícího příkazu:

    ```
    setmqweb properties -k maxMsgTraceFiles -v max
    ```

    kde parametr *max* určuje maximální počet souborů.
  - Pomocí následujícího příkazu resetujte maximální počet souborů, které mají být použity pro trasování systému zpráv, na výchozí hodnotu 5:

    ```
    setmqweb properties -k maxMsgTraceFiles -d
    ```
- Konfigurujte úroveň protokolování, která se používá:
  - Nastavte úroveň protokolování, které se používá, pomocí následujícího příkazu:

    ```
    setmqweb properties -k traceSpec -v level
    ```

    kde *úroveň* je jedna z hodnot vypsaných v Tabulka 52 na stránce 745. Tabulka uvádí úrovně protokolování v podrobné úrovni detailu. Povolíte-li úroveň protokolování, povolíte před ní také úroveň jednotlivých úrovní protokolování. Pokud například povolíte úroveň protokolování produktu ***=warning** , povolíte také úrovně protokolování produktu ***=severe**a ***=fatal** .

    Změňte tuto hodnotu, když ji služba IBM Service požaduje.
  - Pomocí následujícího příkazu resetujte úroveň protokolování, která se používá k výchozí hodnotě ***=info** :

    ```
    setmqweb properties -k traceSpec -d
    ```

Tabulka 52. Platné úrovně protokolování	
Hodnota	**Úroveň protokolování použita**
* =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 nevracení prostředků).
* =audit	Významná událost ovlivňující stav serveru nebo prostředky
* =info	Obecné informace popisující celkový průběh úlohy
* =konfigurace	Změna nebo stav konfigurace
* =detail	Obecné informace podrobně popisující průběh podúlohy
* =jemná	Trasovací informace-obecné trasování, vstup, výstup a návratové hodnoty metod.
* =podrobnější	Informace o trasování-podrobné trasování
* =nejpodrobnější	Trasovací informace-Podrobné trasování, které obsahuje všechny podrobnosti potřebné k ladění problémů.
* =all	Všechny události jsou protokolovány

Konfigurace tokenu LTPA

Tokeny LTPA lze použít k vyhnutí se požadování jména uživatele a hesla pro každý požadavek na mqweb server. Můžete nakonfigurovat název souboru cookie tokenu LTPA, interval vypršení platnosti pro tokeny ověřování LTPA a konfigurovat, zda mohou být tokeny LTPA použity připojením HTTP, 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/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Poznámka: Používáte-li jak IBM MQ Console, tak i ověření tokenu s REST API, interval vypršení platnosti je sdílený.

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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 se uživatelé přihlašují do produktu IBM MQ Console, vygeneruje se token LTPA. Pokud používáte ověření založené na tokenech se serverem REST API, vygeneruje se token LTPA, když se uživatel přihlásí pomocí prostředku `/login` REST API s metodou HTTP POST. Tento token je vrácen v souboru cookie. Token se používá k ověření totožnosti uživatele, aniž by byl uživatel povinen se znovu přihlásit pomocí svého ID uživatele a hesla, dokud nebude platnost tokenu ukončena. Výchozí interval vypršení platnosti je 120 minut.

Název souboru cookie, který obsahuje token LTPA se liší podle platformy:

- MQ Appliance Na serveru IBM MQ Applianceje token LTPA `LtpaToken2`. Tuto hodnotu nelze změnit.
- ULW z/OS Ve výchozím nastavení na všech ostatních platformách se název souboru cookie, který obsahuje token LTPA, spustí s produktem `LtpaToken2`, a obsahuje příponu, která se může změnit při restartu serveru mqweb. Tento náhodný název souboru cookie umožňuje spuštění více než jednoho parametru mqweb na stejném systému. Pokud však chcete, aby název souboru cookie zůstal konzistentní hodnotou, můžete zadat název, který má soubor cookie použít, pomocí příkazu **setmqweb** .

ULW z/OS IBM i Povolíte-li porty HTTP i HTTPS, lze pro požadavek HTTP znovu použít token LTPA, který je vydán pro požadavek HTTPS. Toto chování je při výchozím nastavení vypnuto, ale toto chování lze aktivovat pomocí příkazu **setmqweb** .

Procedura

- Zobrazte aktuální dobu platnosti tokenu LTPA, název souboru cookie tokenu LTPA a zda lze token LTPA použít pro požadavky HTTP, pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  - V poli `ltpaCookieName` je uveden název souboru cookie tokenu LTPA. Pokud jste nenastavili název souboru cookie, hodnota této vlastnosti je `LtpaToken2_${env.MQWEB_LTPA_SUFFIX}` na UNIX, Linux, and Windows , nebo `LtpaToken2_${httpsPort}` na z/OS, . Proměnná za předponou `LtpaToken2_` je používána serverem mqweb k vygenerování jedinečného názvu pro soubor cookie. You cannot set this variable, but you can change the `ltpaCookieName` to a value of your choosing.
  - V poli `ltpaExpiration` je zobrazen čas vypršení platnosti tokenu LTPA.
  - Pokud lze tokeny LTPA používat v požadavcích HTTP, je pole `secureLtpa` nastaveno na hodnotu `false` .

  Další informace viz dspmqweb.
- Nakonfigurujte dobu platnosti tokenu LTPA:
  - Vypršení platnosti tokenu LTPA nastavte zadáním následujícího příkazu:

    ```
    setmqweb properties -k ltpaExpiration -v time
    ```

    , kde parametr *čas* určuje dobu v minutách, po jejímž uplynutí vyprší platnost tokenu LTPA a uživatel je odhlášen.
  - Zadáním následujícího příkazu resetujte vypršení platnosti tokenu LTPA na výchozí hodnotu 120 minut:

    ```
    setmqweb properties -k ltpaExpiration -d
    ```

- ULW z/OS
  Konfigurujte název souboru cookie tokenu LTPA:
  - Nastavte název souboru cookie tokenu LTPA zadáním následujícího příkazu:

    ```
    setmqweb properties -k ltpaCookieName -v name
    ```

    , kde *název* určuje jedinečný název pro soubor cookie tokenu LTPA.
  - Resetujte název souboru cookie tokenu LTPA na výchozí hodnotu, kde předpona `LtpaToken2_` je následována náhodnými znaky zadáním následujícího příkazu:

    ```
    setmqweb properties -k ltpaCookieName -d
    ```
- ULW z/OS
  Zadáním následujícího příkazu nakonfigurujte, zda lze token LTPA použít prostřednictvím připojení HTTP:

  ```
  setmqweb properties -k secureLtpa -v secure
  ```

  kde parametr *secure* určuje, zda lze token LTPA používat jak nezabezpečená připojení HTTP, tak i zabezpečená připojení HTTPS. Hodnota `false` umožňuje, aby připojení HTTP i HTTPS používaly stejný token LTPA.

V 9.1.0 Konfigurace brány administrative REST API

Při výchozím nastavení je brána administrative REST API povolena. Je-li brána administrative REST API povolena, můžete pomocí správce front brány provést vzdálenou administraci s produktem REST API . Správce front, který se používá jako výchozí správce front brány, můžete nakonfigurovat nebo můžete zabránit vzdálené správě zákazem brány administrative REST API pomocí příkazu **setmqweb** .

Informace o této úloze

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Výchozí správce front brány je použit v případě, že jsou splněny obě následující podmínky:

- Správce front není zadán v záhlaví `ibm-mq-rest-gateway-qmgr` požadavku REST.
- Správce front, který je zadán v adrese URL prostředku produktu REST API , není lokálním správcem front.

Další informace o vzdálené administraci s produktem REST APInajdete v tématu Vzdálená administrace pomocí produktu REST API.

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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 brány produktu 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. Další informace viz dspmqweb.
- Pomocí následujícího příkazu nakonfigurujte, zda je brána administrative REST API povolena:

  ```
  setmqweb properties -k mqRestGatewayEnabled -v enabled
  ```

  kde *enabled* je hodnota **true** , která povoluje bránu administrative REST API , nebo **false** jinak.
- Nastavit, který správce front se použije 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 v rámci stejné instalace jako je mqweb server.
  - Zrušte nastavení výchozího správce front brány s použitím následujícího příkazu:

    ```
    setmqweb properties -k mqRestGatewayQmgr -d
    ```

V 9.1.0 Konfigurace messaging REST API

Server mqweb, který je hostitelem produktů IBM MQ Console a REST API , je ve výchozím nastavení aktivován messaging REST API . V 9.1.2 Připojení k produktu IBM MQ ze serveru messaging REST API se sloučí s 20 připojeními, která jsou k dispozici pro každého správce front. Když jsou všechna připojení používána, vytvoří produkt messaging REST API nové připojení, které není ve fondu, pro použití pro požadavek. Můžete změnit maximální počet připojení ve fondu a chování produktu messaging REST API , pokud jsou všechna připojení používána, pomocí příkazu **setmqweb properties** . Můžete také konfigurovat, zda je systém zpráv povolen, pomocí příkazu **setmqweb properties** .

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/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Chcete-li použít messaging REST API , volající musí být ověřen na serveru mqweb a musí být členem role produktu `MQWebUser` . Role `MQWebAdmin` a `MQWebAdminRO` nejsou použitelné pro messaging REST API. Volající musí být také autorizován pro přístup k frontám používaným pro systém zpráv prostřednictvím OAM neboRACF. Další informace o zabezpečení REST APInaleznete v tématu Zabezpečení produktů IBM MQ Console a REST API.

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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 konfigurovat, zda je systém zpráv povolen, pomocí příkazu **setmqweb properties** .

V 9.1.2 Chcete-li optimalizovat výkon produktu messaging REST API, jsou připojení ke správcům front produktu IBM MQ sdílena. To znamená, že místo každého požadavku REST, který vytváří, používá a ruší své vlastní připojení, každý požadavek REST používá připojení z fondu připojení. Při výchozím nastavení je pro každý fond správců front k dispozici 20 připojení a v případě použití všech připojení existují tři možnosti zpracování:

- messaging REST API může vytvořit nové, nesdílené připojení, které se použije pro požadavek. Toto chování je výchozí chování.
- messaging REST API může vrátit chybu.
- Produkt messaging REST API může čekat, až bude připojení ve fondu k dispozici. Tohle čekání je nekonečná čekací doba.

Můžete změnit maximální počet připojení ve fondu a výchozí chování produktu messaging REST API , pokud jsou všechna připojení používána, pomocí příkazu **setmqweb properties** .

Procedura

- Zobrazte aktuální konfiguraci HTTP messaging REST API pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestMessagingEnabled` udává, zda je povoleno messaging REST API . Hodnota je `True` je povolena messaging REST API , nebo `False` jinak. Další informace viz dspmqweb.
- Nakonfigurujte produkt messaging REST API pomocí následujícího příkazu:

  ```
  setmqweb properties -k mqRestMessagingEnabled -v enabled
  ```

  kde *enabled* je hodnota `true` , pokud chcete messaging REST API povolit, nebo `false` jinak.
- V 9.1.2

  Konfigurace fondů připojení pro produkt messaging REST API:
  - Nakonfigurujte maximální velikost fondu připojení pro každý fond správců front pomocí následujícího příkazu:

    ```
    setmqweb properties -k mqRestMessagingMaxPoolSize -v size
    ```

    kde parametr *velikost* určuje velikost fondu.

    Poznámka: Pokud byla nastavena velká hodnota pro *mqRestMessagingMaxPoolSize* a je k ní připojen velký počet správců front, měli byste zvážit zvýšení maximální velikosti haldy mqweb serveru.

    Další informace najdete v tématu Vyladění prostředí JVM mqweb server .
  - Konfigurujte chování serveru messaging REST API , když se všechna připojení v rámci fondu používají následujícím příkazem:

    ```
    setmqweb properties -k mqRestMessagingFullPoolBehavior -v action
    ```

    kde *akce* uvádí akci, která se má provést. *akce* může mít jednu z následujících hodnot:

    blok
    Jakmile budou všechna připojení ve fondu používána, počkejte, až bude připojení k dispozici.

    chyba
    Když se všechna připojení ve fondu používají, vraťte chybu.

Přetečení
Když jsou používána všechna připojení ve fondu, vytvořte připojení mimo fond k použití a po jeho použití se zlikviduje připojení.

V 9.1.0 Konfigurace produktu REST API for MFT

LTS Ve výchozím nastavení nemá server mqweb, který je hostitelem produktů IBM MQ Console a služeb REST, povoleno MFT . Můžete konfigurovat, zda je aktivována služba REST API pro produkt MFT , nastavit koordinačního správce front a zadat časový limit opětného připojení MFT pomocí příkazu **setmqweb properties** . V 9.1.2 Pro příkaz create REST API , jako je **Create transfer** , je třeba přidat `mqRestMftCommandQmgr`. V 9.1.4 CD Webový server, který je hostitelem produktů IBM MQ Console a služeb REST, ve výchozím nastavení MFT nepodporuje.

Než začnete

V 9.1.4 Potřebujete:

- Chcete-li využívat služeb REST produktu MFT , je třeba povolit službu REST produktu MFT nastavením hodnoty **mqRestMftEnabled** na hodnotu *true* a také nastavit název správce front příkazů na hodnotu `mqRestMftCoordinationQmgr`:

```
setmqweb properties -k mqRestMftEnabled -v true
setmqweb properties -k mqRestMftCoordinationQmgr -v <coordinationQmgrName>
```

- Chcete-li odeslat požadavek, vytvořit požadavek, například vytvořit přenos nebo monitor prostředků, musíte nastavit `mqRestMftCommandQmgr`

```
setmqweb properties -k mqRestMftCommandQmgr -v <commandQmgrName>
```

- Restartujte server mqweb a vynuťte tak hodnoty, které jste právě nastavili, zadáním příkazu **endmqweb** , za nímž následuje příkaz **strmqweb** .
- Zkontrolujte stav webového serveru zadáním příkazu **dspmqweb** .

Chcete-li dokončit tuto úlohu, musíte být uživatelem s určitými oprávněními, abyste mohli použít příkazy **dspmqweb** a **setmqweb**:

- z/OS V systému z/OSje třeba mít oprávnění ke spouštění příkazů **dspmqweb** a **setmqweb** a k zápisu přístupu do souboru `mqwebuser.xml` .
- Multi U všech ostatních operačních systémů musíte být privilegovaný uživatel.

Chcete-li použít produkt REST API for MFT, volající musí být ověřen na serveru mqweb a musí být členem minimálně jednoho z rolí produktu `MFTWebAdmin`nebo `MFTWebAdminRO` .

Upozornění: V 9.1.0 z/OS

Před zadáním příkazu **setmqweb** nebo **dspmqweb** v systému z/OS musíte nastavit proměnnou prostředí WLP_USER_DIR tak, aby proměnná ukazovala na konfiguraci serveru mqweb.

Chcete-li to provést, 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 konfigurujete časový limit REST API pro MFT , všimněte si, že první pokus o opětovné vytvoření připojení se provede bezprostředně po přerušení připojení ke koordinačnímu správci front. Dojde-li k selhání, bude mezi každým pokusem o opětovné připojení existovat interval pěti minut. Proto nastavení hodnoty mezi 0-5 způsobí, že se pouze jeden pokus znovu připojí.

Po vypršení limitu opětovného připojení dojde k dalšímu pokusu o nové připojení, je-li vyvolán některý z prostředků produktu REST API for MFT . Dojde-li k selhání pokusu o opětovné připojení, produkt MFT se znovu pokusí znovu navázat spojení každých pět minut, dokud neuplyne časový limit opětného připojení.

Procedura

- Zobrazte aktuální konfiguraci produktu REST API for MFT pomocí následujícího příkazu:

  ```
  dspmqweb properties -a
  ```

  Pole `mqRestMftEnabled` zobrazuje, zda je povoleno REST API pro MFT . Hodnota je `True` , je-li messaging REST API povolena, nebo `False` jinak.

  V poli `mqRestMftCoordinationQmgr` je uveden název koordinačního správce front.

  V 9.1.2 Pole `mqRestMftCommandQmgr` zobrazuje název správce front příkazů.

  Pole `mqRestMftReconnectTimeoutInMinutes` zobrazuje hodnotu časového limitu opětovného připojení, dokud se služby MFT Transfer Rest nezastaví při pokusu o připojení ke koordinačnímu správci front. Další informace viz dspmqweb.
- Konfigurujte, zda je povoleno REST API pro MFT :
  a) Zadáním následujícího příkazu nakonfigurujte, zda je zapnuto REST API pro MFT :

     ```
     setmqweb properties -k mqRestMftEnabled -v value
     ```

     kde *hodnota* je `true` , pokud chcete povolit REST API pro MFT , nebo `false` jinak.
  b) Restartujte server mqweb zadáním následujících příkazů:

     ```
     endmqweb
     strmqweb
     ```
- Konfigurujte koordinačního správce front, z něhož jsou načítány podrobnosti přenosu:
  a) 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 umístěn na počítači, na kterém je spuštěn server mqweb. Při výchozím nastavení je tento název správce front prázdný. Není-li hodnota nastavena, produkt REST API for MFT nepracuje.
  b) Restartujte server mqweb zadáním následujících příkazů:

     ```
     endmqweb
     strmqweb
     ```
- Nakonfigurujte časový limit v minutách, po jehož uplynutí se produkt REST API for MFT pokusí o připojení ke koordinačnímu správci front:
  a) Konfigurujte časový limit pomocí jednoho z následujících příkazů:
     – Nastavte časový limit:

       ```
       setmqweb properties -k mqRestMftReconnectTimeoutInMinutes -v time
       ```

       kde *čas* uvádí čas, v minutách, před vypršením časového limitu.

       Je-li tato hodnota nastavena mezi `0-5`, REST API se pro MFT pokusí znovu připojit ke koordinačnímu správci front pouze jednou. Pokud připojení selže, nejsou žádné pokusy o opětovné navázání připojení, dokud nebude vyvolán REST API .

Je-li tato hodnota nastavena na `-1`, REST API se pro MFT pokusí znovu navázat spojení, dokud nebude připojení úspěšné.

– Reset časového limitu na výchozí hodnotu 30 minut:

```
setmqweb properties -k mqRestMftReconnectTimeoutInMinutes -d
```

b) Restartujte server mqweb zadáním následujících příkazů:

```
endmqweb
strmqweb
```

- V 9.1.2 Konfigurujte správce front příkazů pro vytvoření požadavku:

a) Nakonfigurujte správce front příkazů pomocí následujícího příkazu:

```
setmqweb properties -k mqRestMftCommandQmgr -v qmgrName
```

kde *qmgrName* je název správce front příkazů. Správce front příkazů musí být na počítači, na kterém je spuštěn server mqweb. Při výchozím nastavení je tento název správce front prázdný. Není-li hodnota nastavena, MFT REST API pro příkaz create nefunguje.

b) Restartujte server mqweb zadáním následujících příkazů:

```
endmqweb
strmqweb
```

V 9.1.0 Vyladění prostředí JVM serveru mqweb

Standardně používá prostředí JVM (Java Virtual Machine) serveru mqweb 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:

   - ULW V systému UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - 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.
2. Volitelné: Nastavte maximální velikost haldy přidáním následujícího řádku do souboru:

   ```
   -Xmx<MaxSize>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:

   ```
   -XscmxSizem
   ```

   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. Volitelné: Nastavte kódování souboru, které se používá pro informace o konfiguraci řídicího panelu uživatele v souboru IBM MQ Console přidáním následujícího řádku do souboru:

   ```
   -Dfile.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 souborů instalační komponenty produktů IBM MQ Console a REST API

Existují dvě sady adresářových struktur, které jsou přidruženy k instalační komponentě produktů IBM MQ Console a REST API . Jedna adresářová struktura obsahuje soubory, které lze upravovat. Druhá adresářová struktura obsahuje soubory, které nelze upravit.

upravitelné soubory

Upravitelné soubory uživatele jsou umístěny jako součást počáteční instalace instalační komponenty produktu IBM MQ Console a produktu REST API . Vzhledem k tomu, že tyto soubory lze upravit, soubory se při použití údržby nemění.

Umístění upravitelných souborů uživatele závisí na operačním systému:

- ULW V systému UNIX, Linux, and Windows: *MQ_DATA_PATH*/web/installations/*installationName*/
- IBM i V systému IBM i: *MQ_DATA_PATH*/web/installations/Installation1/
- z/OS V systému z/OS: *WLP_user_directory*

  kde *WLP_user_directory* je adresář, který byl zadán při spuštění skriptu V 9.1.0 **crtmqweb** za účelem vytvoření definice mqweb serveru.

Pod tímto adresářem nejvyšší úrovně jsou přítomny následující adresáře a soubory:

Adresáře a soubory	Popis
angular.persistence/	Adresář, kde je uložena konfigurace panelu dashboard produktu IBM MQ Console .
servers/	Adresář serverů profilu WebSphere Liberty .
servers/mqweb	Adresář, který obsahuje adresářovou strukturu mqweb serveru.
servers/mqweb/logs	Adresář, který obsahuje protokoly pro protokol mqweb.
servers/mqweb/logs/console.log	Protokol základního stavu serveru a zpráv operace.
servers/mqweb/logs/ffdc	Výstupní adresář FFDC (First Failure Data Capture).
servers/mqweb/logs/messages.log	Protokol běhových zpráv z mqweb serveru, včetně IBM MQ Console a REST API. Starší zprávy jsou uloženy v souborech, které se nazývají messages_*timestamp*.log.
servers/mqweb/logs/trace.log	Protokol trasování z mqweb serveru, včetně IBM MQ Console a REST API. Starší trasování je uloženo v souborech, které se nazývají 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	Konfigurační soubor hlavního serveru. Tento soubor je určen pouze pro čtení. Chcete-li přepsat výchozí konfiguraci, upravte soubor mqwebuser.xml .
servers/mqweb/mqwebuser.xml	Konfigurační soubor pro IBM MQ Console a REST API. Nastavení, která jsou konfigurovaná v tomto souboru, přepíší výchozí konfiguraci. Chcete-li upravit tento soubor, musíte být privilegovaný uživatel .
servers/mqweb/resources	Adresář, který obsahuje různé prostředky serveru, jako např. úložiště klíčů.

Adresáře a soubory	Popis
`servers/mqweb/workarea`	Adresář, který je vytvořen serverem při provozu. Tento adresář je vytvořen po prvním spuštění serveru.

Neupravitelné soubory

Neupravitelné soubory jsou umístěny jako součást počáteční instalace instalační komponenty produktů IBM MQ Console a REST API . Tyto soubory se aktualizují, když se použije údržba.

Umístění upravitelných souborů uživatele závisí na operačním systému:

- ULW V systému UNIX, 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 produktu IBM MQ UNIX System Services Components.

V tomto umístění jsou přítomna následující adresářová struktura a soubory:

Adresáře a soubory	Popis
`bin/`	Adresář, který obsahuje příkazy Liberty. Chcete-li spouštět skripty v tomto adresáři, musíte být privilegovaný uživatel .
`mq/`	Adresářová struktura, která obsahuje různé prostředky produktu IBM MQ .
`mq/apps/`	Adresář, který obsahuje aplikace IBM MQ Console a REST API .
`mq/etc/`	
`mq/etc/mqweb.xml`	Konfigurační soubor pouze pro čtení pro server mqweb. Upravte soubor `mqwebuser.xml` a proveďte změny konfigurace.
`mq/libs`	Adresář, který obsahuje sdílené knihovny určené pro použití v produktu 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` .

V 9.1.0 z/OS Konfigurace záznamu použití webového serveru mqweb v systému z/OS

Chcete-li určit použití produktu, systém z/OS zaznamená množství času procesoru, které je používáno aplikačním serverem mqweb, který je hostitelem produktů IBM MQ Console a REST API. Je možné, že bude třeba nakonfigurovat server mqweb, aby zaznamenáváte použití pro správné ID produktu.

Než začnete

Chcete-li dokončit tento postup, musíte mít oprávnění k odpojení a připojení souborových systémů a zastavení a restartování spuštěné úlohy mqweb server.

Informace o této úloze

Při výchozím nastavení je použití parametru mqweb serveru zaznamenáno jako samostatný produkt IBM MQ for z/OS s ID produktu 5655-MQ9. Pokud jste licencováni pro použití produktu IBM MQ for z/OS Value Unit Edition (VUE)nebo IBM MQ Advanced for z/OS Value Unit Edition, musíte za tímto postupem změnit ID produktu, pro které je zaznamenáno použití serveru mqweb.

Ve všech následujících krocích nahraďte následující kroky:

- WLP_USER_DIR s názvem uživatelského adresáře protokolu Liberty, který byl původně předán produktu **crtmqweb**, také známý pod názvem 'USERDIR' v proceduře JCL webového serveru.
- `PathPrefix` s názvem instalační cesty komponent produktu IBM MQ for z/OS UNIX System Services (USS).

Postup

1. V prostředí USS vytvořte nový adresář '`mqweb_extension`' v adresáři WLP_USER_DIR.
   Příklad:

```
mkdir /var/mqm/web/installation1/mqweb_extension
```

2. Vytvořte soubor ASCII s názvem `mqweb.properties` v adresáři `WLP_USER_DIR/mqweb_extension` .
3. Upravte soubor `mqweb.properties` tak, aby obsahoval řádek:

```
com.ibm.websphere.productInstall= WLP_USER_DIR/mqweb_extension
```

   Také přidejte jednu z následujících tří čar, které se odkazují na PID zaznamenaného produktu:

   `com.ibm.websphere.productId=com.ibm.mq`nebo
   `com.ibm.websphere.productId=com.ibm.mqvue`nebo
   `com.ibm.websphere.productId=com.ibm.mqadv`

4. V prostředí USS vytvořte adresář `WLP_USER_DIR/mqweb_extension/lib/features/`.
   Použijte například příkaz USS

```
mkdir -p WLP_USER_DIR/mqweb_extension/lib/features/
```

5. V prostředí USS vytvořte adresář `WLP_USER_DIR/mqweb_extension/lib/versions/`.
   Použijte například příkaz USS

```
mkdir -p WLP_USER_DIR/mqweb_extension/lib/versions/
```

6. Zkopírujte jeden z následujících souborů z `PathPrefix/web/mq/etc` na `WLP_USER_DIR/mqweb_extension/lib/versions`.
   Soubor, který potřebujete zkopírovat, závisí na typu produktu, který chcete konfigurovat pro záznam použití.

   `mq.properties`
   Použití webového serveru mqweb se zaznamenává jako samostatný produkt IBM MQ for z/OS s ID produktu 5655-MQ9.

   `mqVue.properties`
   Použití webového serveru mqweb se zaznamenává jako samostatný produkt IBM MQ for z/OS Value Unit Edition (VUE) s ID produktu 5655-VU9.

   `mqAdvancedVue.properties`
   Použití webového serveru mqweb se zaznamenává jako část produktu IBM MQ Advanced for z/OS Value Unit Edition s ID produktu 5655-AV1.

7. Je-li zaznamenané použití serveru mqweb pro ID produktu 5655-VU9 nebo ID 5655-AV1, upravte soubor vlastností v adresáři `WLP_USER_DIR/mqweb_extension/lib/versions` .

   Proveďte to nahrazením řádku

```
com.ibm.websphere.productReplaces=com.ibm.websphere.appserver.zos
```

   s čárou

```
com.ibm.websphere.productReplaces=com.ibm.mq
```

8. V adresáři `WLP_USER_DIR/servers/mqweb`upravte soubor `server.env` a přidejte následující řádek:

```
WLP_PRODUCT_EXT_DIR=WLP_USER_DIR/mqweb_extension
```

9. Změňte vlastnictví a oprávnění adresářů a souborů v uživatelském adresáři Liberty tak, aby náležely k ID uživatele a skupině, pod kterou pracuje mqweb server.

   Použijte tyto příkazy:

```
chown -R userid:group WLP_USER_DIR
chmod -R 770 WLP_USER_DIR
```

10. Je-li spuštěn server mqweb, zastavte server pomocí příkazu MVS **STOP** na spuštěné úloze mqweb server.
11. Připojte systém souborů produktu IBM MQ for z/OS UNIX System Services Components pro přístup pro čtení a zápis pomocí příkazu TSO/E **MOUNT** s parametrem **MODE(RDWR)** .
12. Odstraňte všechny následující soubory z adresáře *PathPrefix*`/web/lib/versions` :
    - `mq.properties`
    - `mqVue.properties`
    - `mqAdvancedVue.properties`
13. Zkopírujte `PathPrefix/web/mq/etc/mq.properties` do adresáře `PathPrefix/web/lib/versions`.

    Tento výchozí soubor vlastností může být přepsán v závislosti na zaznamenaném produktu, ale je povinný.
14. Připojte systém souborů IBM MQ for z/OS UNIX System Services Components pro přístup jen pro čtení pomocí příkazu TSO/E **MOUNT** s parametrem **MODE(READ)** .
15. Spusťte mqweb server pomocí příkazu MVS **START** *procname* , kde *procname* je název procedury spuštěné úlohy mqweb serveru.
16. V adresáři `messages.log`, v adresáři `WLP_USER_DIR/servers/mqweb/logs`, zpráva CWWKB0108I ověřuje zaznamenaný produkt.

    Příklad:

```
CWWKB0108I: IBM CORP product MQM MVS/ESA version V9 R1.0 successfully registered with z/OS.
```

V 9.1.4 MQ Adv. Linux MQ Adv. VUE Definování připojení Aspera gateway v systému Linux

Produkt IBM Aspera fasp.io Gateway poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě IBM MQ. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux.

Informace o této úloze

Aspera gateway lze použít ke zlepšení výkonu kanálů správce front. Je zvláště efektivní, má-li síť vysokou latenci nebo má tendenci ztrácet pakety, a obvykle se používá k urychlení připojení mezi správci front v různých datových centrech.

Poznámka: Pro rychlou síť, která neztratí pakety, je snížení výkonu při použití Aspera gateway, takže je důležité zkontrolovat výkon sítě před definováním připojení Aspera gateway a po něm.

Definujete Aspera gateway na každém konci síťového připojení IP a potom pomocí protokolu TCP/IP připojíte kanály správce front ke každé komunikační bráně. Správce front nemusí být spuštěn ve stejném počítači jako produkt Aspera gateway , který používá, a více správců front může používat stejnou bránu. Jediná omezení jsou následující:

Chcete-li použít produkt Aspera gateway, musíte mít jeden nebo více z následujících oprávnění:

- IBM MQ Advanced for Multiplatforms
- IBM MQ Appliance
- V 9.1.5 IBM MQ Advanced for z/OS VUE

Produkt Aspera gateway můžete implementovat na libovolné z následujících platforem Linux (Red Hat nebo Ubuntu):

- Linux for x86-64
- V 9.1.5 Linux on POWER Systems - Little Endian
- V 9.1.5 Linux for IBM Z

Použití produktu Aspera gateway je omezeno na zprávy produktu IBM MQ , pokud není brána samostatně oprávněna.

Správci front, kteří používají produkt Aspera gateway , mohou být spuštění na libovolné oprávněné platformě, která je podporována pro vydání produktu Continuous Delivery (CD). Úplný seznam platforem produktu CD naleznete v tématu Ikony vydání a platformy v dokumentaci produktu.

Pro každého správce front, který se nenachází ve stejném počítači jako produkt Aspera gateway , který používá, zkontrolujte, zda mezi správcem front a produktem Aspera gatewayexistuje rychlé síťové připojení.

Soubor `toml` se používá k vytvoření definice brány, která definuje příchozí a odchozí porty, které brána používá. Ukázkový soubor `toml` se dodává spolu s Aspera gateway. Definice odchozí brány definuje připojení z lokálního správce front k bráně a z lokální brány do vzdálené brány. Definice příchozí brány definuje připojení ze vzdálené brány k lokální bráně a z lokální brány do lokálního správce front.

Následující kroky poskytují základní příručku k získání a spuštění. Další podrobné informace viz dokumentace IBM Aspera fasp.io Gateway V1.0.0.

Postup

1. Získejte instalační obraz produktu Aspera gateway .

   Pokud má váš podnik oprávnění IBM MQ Advanced for Multiplatforms nebo IBM MQ Appliance , můžete stáhnout Aspera gateway z programu Passport Advantage, jako "IBM MQ V9.1.x Continuous Delivery Release for IBM Aspera fasp.io eAssembly ". Chcete-li stáhnout toto eAssembly, přejděte na Stahování IBM MQ 9.1 a poté klepněte na kartu pro nejnovější vydání souvislého doručení. eAssembly obsahuje instalační obrazy pro všechny platformy Linux , na kterých je brána k dispozici.

   V 9.1.5 Má-li váš podnik oprávnění k produktu IBM MQ Advanced for z/OS VUE , můžete získat Aspera gateway z komponenty konektoru Connector, která je součástí instalace SMP/E. Další informace naleznete v adresáři programu IBM MQ Advanced for z/OS VUE (IBM MQ for z/OS Program Directory Directory PDF). Je-li balík konektoru nainstalován, vytvoří adresář fap v systémových službách systému

Unix, který obsahuje soubor `.zip` . Soubor `.zip` obsahuje instalační obrazy pro všechny platformy Linux , na kterých je brána k dispozici. Všimněte si, že Aspera gateway nelze spustit nativně na z/OS.

2. Zkopírujte obraz instalace produktu Aspera gateway do dvou počítačů, které spustí bránu, a poté extrahujte a nainstalujte bránu.

   Instalace pomocí produktu RPM Package Manager (RPM):

   ```
   rpm -ivh ibm-fasp.io-gateway-1.0.0_qa_48-1.x86_64.rpm
   ```

   Chcete-li instalovat pomocí RPM na systému Ubuntu, máte dvě možnosti:

   - Přidejte atribut `--force-debian` do instalačního příkazu Aspera gateway , jak je vysvětleno v tématu Instalace klienta IBM MQ na Linux pomocí rpm.
   - Použijte příkaz apt-get:

     ```
     sudo apt-get install ./ibm-fasp.io-gateway_1.0.0_amd64.deb
     ```

3. Nakonfigurujte každou bránu.

   Upravte soubory `gateway.toml` a `logging.toml` v adresáři `/etc/fasp.io` , který byl vytvořen instalací. Použijte soubor `gateway.toml` k definování příchozích a odchozích portů, které brána používá, a soubor `logging.toml` k definování úrovně protokolování, které požadujete. Příklad pro úpravu souborů `gateway.toml` je uveden dále v tomto tématu.

4. Na každém konci síťového připojení změňte definici kanálu tak, aby se připojovala k portu, na kterém lokální komunikační brána naslouchá.
5. Spusťte každou službu brány.
   Z příkazového řádku spusťte tento příkaz:

   ```
   systemctl start fasp.io-gateway
   ```

6. Restartujte kanály.

   Tito správci front nyní komunikují prostřednictvím připojení produktu Aspera gateway .

Příklad

Tento příklad definuje připojení Aspera gateway na dvou počítačích se systémem Linux. Konfigurace je následující:

- Adresa IP počítače lokální 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 se změní tak, aby se připojil k lokálnímu serveru Aspera gateway pomocí **conname** 9.20.193.107(1500). Kanál správce front na vzdáleném správci front se změní tak, aby se připojil ke vzdálenému serveru Aspera gateway pomocí **conname** 9.20.192.115(1500).

1. Definujte připojení Aspera gateway na lokálním počítači brány:

   - Nainstalujte Aspera gateway:

     ```
     rpm -ivh ibm-fasp.io-gateway-1.0.0_qa_48-1.x86_64.rpm
     ```

   - Upravte soubor `gateway.toml` v adresáři `/etc/fasp.io` , který byl vytvořen instalací. Upravte jej, chcete-li nastavit definice lokální brány.

     ```
     [[bridge]]
         name = "Outbound"
         [bridge.local]
                protocol = "tcp"
                    host = "9.20.193.107"
                    port = 1500

         [bridge.forward]
     ```

```
            protocol = "fasp"
                host = "9.20.192.115"
                port = 1600

[[bridge]]
    name = "Inbound"
    [bridge.local]
            protocol = "fasp"
                host = "9.20.193.107"
                port = 1600

    [bridge.forward]
            protocol = "tcp"
                host = "9.20.121.5"
                port = 1414
```

2. Opakováním předchozího kroku definujte připojení produktu Aspera gateway na vzdáleném počítači brány. Upravte soubor `gateway.toml` v adresáři `/etc/fasp.io` , který byl vytvořen instalací. Upravte jej, chcete-li nastavit definice vzdálených bran:

```
[[bridge]]
    name = "Outbound"
    [bridge.local]
            protocol = "tcp"
                host = "9.20.192.115"
                port = 1500

    [bridge.forward]
            protocol = "fasp"
                host = "9.20.193.107"
                port = 1600

[[bridge]]
    name = "Inbound"
    [bridge.local]
            protocol = "fasp"
                host = "9.20.192.115"
                port = 1600

    [bridge.forward]
            protocol = "tcp"
                host = "9.20.121.25"
                port = 1414
```

3. Na každém konci připojení změňte definici kanálu tak, aby se připojovala k portu, na kterém lokální brána naslouchá.
   - Změňte kanál správce front na lokálním správci front tak, aby se připojoval k lokálnímu serveru Aspera gateway pomocí **conname** 9.20.193.107(1500).
   - Změňte kanál správce front na vzdáleném správci front tak, aby se připojil ke vzdálenému serveru Aspera gateway pomocí **conname** 9.20.192.115(1500).
4. Spusťte lokální bránu spuštěním následujícího příkazu na počítači lokální brány:

```
systemctl start fasp.io-gateway
```

5. Spusťte vzdálenou bránu spuštěním následujícího příkazu na vzdáleném počítači brány:

```
systemctl start fasp.io-gateway
```

6. Restartujte kanály.

Jak pokračovat dále

Produkt Aspera gateway předává data, která přijímá, aniž by to jakýmkoli způsobem interpretoval. To znamená, že můžete nakonfigurovat TLS mezi kanály správce front, které používají produkt Aspera gateway, protože připojení brány netuší o navázání komunikace TLS. To také znamená, že správci front na všech podporovaných platformách IBM MQ mohou používat produkt Aspera gateway.

Chcete-li použít správce front s více instancemi s branou, nakonfigurujte definice bran pro každou instanci správce front.

Poznámka: Produkt Aspera gateway byl otestován pouze s kanály správce front. Nebyl testován s kanály klienta. Je to proto, že předpokládané použití pro Aspera gateway je pro připojení vzdálených správců front přes pomalou síť, zatímco aplikace klienta se obvykle připojují ke správcům front v místním datovém centru přes rychlou síť.

Související odkazy

Orientační plán analyzátoru Aspera gateway

“Který typ komunikace použít” na stránce 15

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

Dokumentace k produktu IBM Aspera fasp.io Gateway V1.0.0

V 9.1.0 Multi Konfigurace IBM MQ pro použití se IBM Cloud Private službou měření

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 (formerly Bluemix) . 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.

V 9.1.1 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` (dříve `BluemixRegistration`) 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:

```
4/22/2018 01:44:29 PM - Process(1274.1) User(bld-adm) Program(amqmgr0)
Host(8b3b83f2bc7d) Installation(Docker)
VRMF(9.1.0.0)
Time(2018-04-22T13:44:29.295Z)
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.

V 9.1.1 **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
Adresa 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 pojmy
Metrika cen pro virtuální jádra procesoru (VPC)

V 9.1.1 Multi Konfigurace správce front pro použití s instancí měřicích služeb v systému IBM Cloud Private

Nastavte informace o zabezpečení a registraci produktu IBM Cloud pro správce front a poté se připojte k instanci měřicího služby, kterou jste již vytvořili.

Informace o této úloze

Řídicí panel instance Měřicí službaIBM Cloud Private zobrazuje data pouze pro správce front, kteří jsou nakonfigurováni, aby zahrnuli informace o zabezpečení a registraci IBM Cloud Private .

Postup

1. Při vytváření ID služby postupujte podle pokynů uvedených v dokumentu ICP dokumentovaných kroků:

   Vytvoření ID služby pomocí rozhraní CLI produktu IBM Cloud Private.
2. Při vytváření klíče rozhraní API postupujte podle dokumentovaných kroků ICP na:

   Rozhraní API pro správu klíčů rozhraní API.
3. Stáhněte si certifikáty TLS z klastru ICP.

   Poznamenejte si umístění, kam jste stáhli certifikáty. Stáhnuté certifikáty můžete přidat do úložiště klíčů pro vašeho správce front v kroku “9” na stránce 763.
4. Vytvořte textový soubor `apikeyfile.txt` a přidejte hodnotu do pole **`API key`** , kterou jste zkopírovali v předchozí úloze.

   Poznamenejte si umístění produktu `apikeyfile.txt` , abyste do něj mohli zahrnout cestu v kroku 8. Tento soubor musí být čitelný pro uživatele správce front (*'mqm*' na systémech UNIX). Soubor musí obsahovat pouze samotný **`API key`** , ne 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 více platformách.
6. Spusťte správce front *QM1*.

   Další informace naleznete v tématu Spuštění správce front.
7. Nezapomeňte nastavit prostředí příkazového řádku produktu IBM MQ před spuštěním příkazů 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 zabezpečení SSL pro správce front *QM1*.

   AIX Začněte vytvářet úložiště údajů o důvěryhodnosti, na AIX:Amend pro systém 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 763, 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` do souboru `qm.ini` správce front:

```
ReportingService:
   APIKeyFile=APIKey file location/apikeyfile.txt
```

11. Přidejte hodnotu **API host** do souboru `qm.ini` .

    Sekce 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 pro proces správce front **amqzmur0** pro přístup k síti. K povolení správce front je nutný přístup, aby mohl být kontaktován měřič služby.

13. Zobrazte informace o správci front *QM1* ve své instanci měřicího služby.

    Když je stav vykazování aktivní, informace o spuštění a použití pro všechny integrační servery na uvedeném uzlu integrace se hlásí do služby měření. Informace o použití se aktualizují každých 15 minut.

14. Volitelné: Zastavte správce front z vytváření sestav do služby měření odebráním oddílu `ReportingService` ze souboru `qm.ini` správce front a znovu spusťte správce front.

15. Volitelné: Zkontrolujte diagnostické informace v souboru protokolu správce front, pokud se správce front nezdaří nahlásit spuštění nebo informace o použití do služby měření.

    Amend 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 tak, aby se připojoval k instanci. Informace o správci front v řídicím panelu instance služby měření si můžete prohlédnout.

V 9.1.1 Multi Připojení k měřicím službám IBM Cloud Private přes proxy HTTP

Je-li správce front spuštěn v systému, který nemá přímý přístup ke svému klastru ICP, můžete použít server proxy HTTP, který vaše organizace poskytuje pro připojení k instanci služby měření v produktu IBM Cloud Private.

Než začnete

Nakonfigurovali jste zabezpečení, jste přidali adresu URL produktu **API key** a adresu URL služby do souboru `qm.ini` pro správce front.

Informace o této úloze

Pomocí této úlohy nakonfigurujete správce front tak, aby se připojil k instanci měřící služby v produktu IBM Cloud Private prostřednictvím serveru proxy HTTP, který je poskytován vaší organizací.

Procedura

- Přidejte atribut zástupce služby do stanzy registrace IBM Cloud Private vašeho souboru `qm.ini` .
  Atribut **ServiceProxy** můžete nastavit takto:
  - Adresa URL, která obsahuje předponu http:// a volitelně port. Pokud neuvedete port, použije se *1080* .

    ```
    ReportingService:
       ServiceProxy=http://myorgproxy.net:1080
    ```

  Poznámka: Parametr **ServiceProxy** musí být nastaven na platnou adresu URL http://. Další protokoly serveru proxy, například HTTPS a SOCKS, nejsou podporovány.
- Restartujte správce front, aby se změny projevily.

V 9.1.1 Multi Odstraňování problémů s připojením k měřidle služby

Odstraňování problémů s chybami, se kterými se můžete setkat při připojování správce front k instanci služby měření.

Správce front se nemůže registrovat nebo odesílat metriky využití do konfigurované služby měření

Zkontrolujte, zda má správce front přístup k síti. Hodnota **APIKey** v souboru s klíči API je nesprávná. Ujistěte se, že je komponenta GSKit nainstalována.

Neplatná stanza `qm.ini`

Byla nalezena neplatná sekce `qm.ini` . Další informace naleznete v protokolu chyb.

Neplatný parametr proxy služby HTTP

Hodnota atributu **ServiceProxy** pro objekt stanza správce front `ReportingService` není správně nakonfigurována. Správce front se neregistruje se službou. Parametr **ServiceProxy** musí být nastaven na platnou adresu URL http://. Další protokoly serveru proxy, například HTTPS a SOCKS, nejsou podporovány.

V 9.1.0 Linux Konfigurace produktu IBM MQ pro použití s akcemi typu push platformy Salesforce a událostmi platformy

Tyto informace použijte k nastavení zabezpečení a připojení k produktu Salesforce a vaší síti IBM MQ , a to konfigurací a následným spuštěním IBM MQ Bridge to Salesforce.

Než začnete

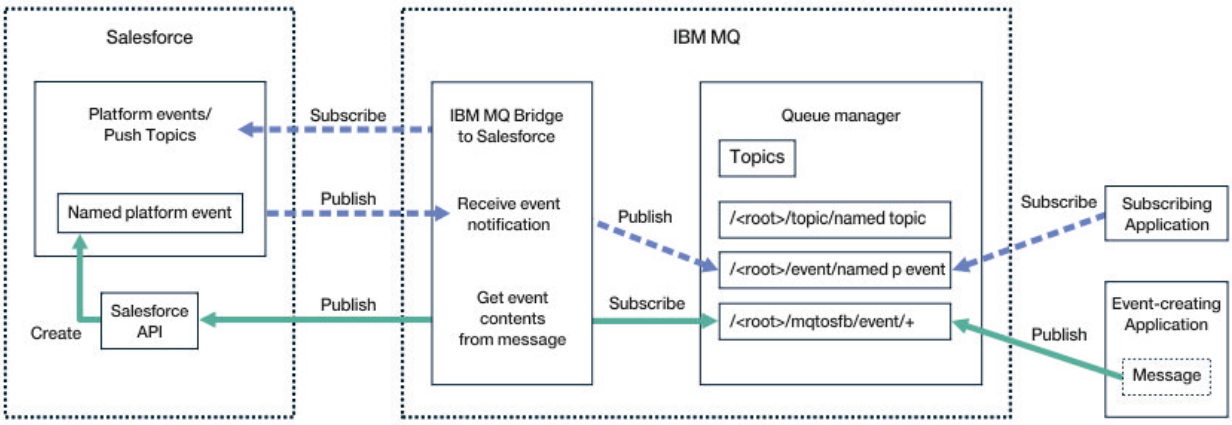
Poznámka: Produkt IBM MQ Bridge to Salesforce je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-431).

- IBM MQ Bridge to Salesforce je k dispozici na Linux pro x86-64 (64 bitů). Most není podporován pro připojení ke správcům front spuštěnému v produktu IBM WebSphere MQ 6.0 a starším.
- V 9.1.2 Produkt IBM MQ 9.1.2 zavádí další volby konfigurace. Hlavní změna spočívá v tom, že správce front může nyní podporovat více instancí mostu, ve kterých byly správně nakonfigurovány. Další informace viz “Další volby konfigurace pro IBM MQ Bridge to Salesforce” na stránce 772.
- Nainstalujte balík produktu **MQSeriesSFBridge** . Další informace naleznete v tématu Instalace serveru IBM MQ v systému Linux.

Informace o této úloze

Salesforce je cloudová platforma pro správu vztahů v cloudu. Pokud používáte produkt Salesforce ke správě zákaznických dat a interakcí, můžete použít produkt IBM MQ Bridge to Salesforce k přihlášení k odběru Salesforce témat a událostí platformy, které lze následně publikovat ve správci front produktu IBM MQ . Aplikace, které se připojují k tomuto správci front, mohou vhodným způsobem spotřebovávat data typu push a platformy událostí platformy. Můžete také použít most k vytvoření zpráv událostí pro události platformy v produktu Salesforce.

Přehled produktu IBM MQ Bridge to Salesforcenaleznete v diagramu 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 hesel typu push a o tom, jak používat rozhraní Streaming API, najdete v části Seznámení se streaming API a Práce s PushTopics.

Události platformy jsou přizpůsobitelné zprávy událostí, které lze definovat za účelem určení dat událostí, která platforma produktu `Force.com` produkuje nebo spotřebovává. Další informace o událostech platformy a rozdílu mezi událostmi produktu Salesforce naleznete v tématu Události platformy Enterprise Messaging a Jaký je rozdíl mezi událostmi Salesforce.

- Chcete-li vytvořit konfiguraci pro přihlášení k odběru témat a událostí platformy, prohlédněte si téma “Konfigurace IBM MQ Bridge to Salesforce” na stránce 767.
- Chcete-li vytvořit konfiguraci pro vytváření zpráv událostí pro události platformy Salesforce , prohlédněte si téma “Vytvoření zpráv událostí pro události platformy Salesforce” na stránce 774.

Data z mostu můžete monitorovat dvěma způsoby pomocí IBM MQ Console a pomocí parametru **`-p`** s příkazem **`amqsrua`** . Jedna sada dat je publikována pro celkový stav mostu:

- Celkový počet zpráv témat typu push, které jsou zpracovány v intervalu (pod stromem `STATUS/PUSHTOPIC`).
- Počet témat typu push, která se zobrazují v tomto intervalu.
- Celkový počet událostí platformy, které jsou zpracovány v intervalu (pod stromem `STATUS/PLATFORM`).
- Počet událostí platformy, které se zobrazují v tomto intervalu.
- Celkový počet IBM MQ vytvořených událostí platformy, které jsou zpracovány v intervalu (pod stromem `STATUS/MQPE`).
- Jedinečný počet IBM MQ vytvořených událostí platformy, které se zobrazují v tomto intervalu.
- Počet nezdařených publikování IBM MQ vytvořených událostí platformy, které jsou v tomto intervalu vidět.

Pro každé konfigurované téma Salesforce je publikována další zpráva. Téma IBM MQ používá úplný název tématu Salesforce a `/event` nebo `/topic` v názvu objektu:

- Počet zpráv, které byly zpracovány v intervalu.

Chcete-li nakonfigurovat produkt IBM MQ Console k monitorování dat mostu, projděte si kroky 9 a 10 v části Konfigurace produktu IBM MQ Bridge to Salesforce. Informace o použití příkazu **`amqsrua`** naleznete v tématu Monitorování produktu IBM MQ Bridge to Salesforce.

Postupujte podle kroků uvedených v těchto úlohách a nakonfigurujte a spusťte IBM MQ Bridge to Salesforce:

Postup

1. Nakonfigurujte agenta IBM MQ Bridge to Salesforce.
2. V 9.1.0
   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 (spuštění produktu IBM MQ Bridge na Salesforce)

V 9.1.0 Linux Konfigurace IBM MQ Bridge to Salesforce

Můžete nakonfigurovat IBM MQ a zadat parametry IBM MQ Bridge to Salesforce pro vytvoření konfiguračního souboru a připojení Salesforce push témat a událostí platformy ke správci front IBM MQ .

Než začnete

Před spuštěním této úlohy se ujistěte, že jste nainstalovali balík produktu `MQSeriesSFBridge` ve své instalaci produktu IBM MQ na platformu x86-64 Linux .

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným k vytvoření konfiguračního souboru IBM MQ Bridge to Salesforce a k úspěšnému připojení k produktu Salesforce a IBM MQ , abyste se mohli přihlásit k odběru Salesforce témat a událostí platformy. Další informace o významu a volbách pro všechny parametry naleznete v popisu příkazu runmqsfb . Musíte zvážit své vlastní požadavky na zabezpečení a přizpůsobit parametry vhodné pro vaši 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 774.

Přihlášení k odběru Salesforce push témat a událostí platformy

Když produkt IBM MQ Bridge to Salesforce ustanoví připojení k produktu Salesforce i IBM MQ, vytvoří odběry pro Salesforce push témat a událostí platformy. Název typu push nebo název události platformy, k níž se most chce přihlásit, je třeba zahrnout do konfiguračního souboru nebo přidat do příkazového řádku před připojením připojení.

Jeden z konfiguračních atributů je kořenem stromu témat IBM MQ a události jsou publikovány pod tímto kořenem. Most přistupuje k tomuto kořenovému adresáři a přidá úplný název tématu produktu Salesforce , například `/MQ/SF/ROOT/topic/EscalatedCases`. Monitorovací téma a aplikace, které se připojují k produktu IBM MQ , mohou hledat témata typu push pod produktem `/topic/EscalatedCases` a události platformy v rámci produktu `/event/NewCustomer__e`.

Publikovaná zpráva obsahuje řídicí informace a strukturu dat, která obsahuje požadovaná datová pole. Pro témata typu push je struktura dat **`sobject`** a pro události platformy je struktura **`payload`**. Most se nemůže přihlásit k odběru tématu nebo události, nejsou-li definovány v produktu Salesforce. Pokud most narazí na chybu při pokusu o přihlášení k odběru tématu, most se zastaví.

Objekt tématu nemusí být definován v produktu IBM MQ , ale musí existovat vhodná oprávnění, která jsou založena na nejbližším nadřazeném prvku ve stromu. Znovu publikovaná zpráva obsahuje ve výchozím nastavení pouze relevantní strukturu dat z původní zprávy. Řídicí informace jsou odebrány. Pro události platformy má publikování strukturu informačního obsahu. Volba konfigurace produktu **`Publish control data with the payload`** v sadě **Chování programu mostu** konfiguračních parametrů umožňuje přepublikování celé zprávy včetně řídicích dat. Další informace viz Konfigurační parametry.

Každá událost typu push a událost platformy má přidružený *ReplayID* na publikaci z produktu 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 přemostění nezmeškat aktuální témata typu push a události platformy i v případě, že nebyla spuštěna v době generování. Most podporuje dvě režimy kvality služby:

At-most-once
: Most nepoužívá volbu *ReplayId* k restartu. Po restartu mostu se zpracují pouze nově vygenerovaná témata typu push a události platformy. Aplikace musí být připraveny se vypořádat s chybějícími publikacemi. *ReplayId* je stále sledováno pomocí mostu a odolný vůči frontě, takže most lze restartovat s jinou kvalitou služby a znát aktuální stav.

Minimálně-jednou
: Položka *ReplayId* je sledována podle mostu a upřesněná ve frontě. Při restartu mostu se trvale uchovává *ReplayId* k požadavku na počáteční bod pro publikování ze serveru. Za předpokladu, že mezera nebyla delší než 24 hodin, jsou zaslány starší publikace. Položka *ReplayId* pro téma není zatvrzená pro každou zprávu. Je zapisován v trvalé zprávě v pravidelných intervalech a je-li přemostění ukončen. Aplikace musí být připraveny k zobrazení duplicitních příruček.

Hodnota *ReplayId* je zapsána jako zpráva do nově definované fronty. Před spuštěním mostu je třeba tuto frontu definovat **`SYSTEM.SALESFORCE.SYNCQ`**. Pokud **`SYSTEM.SALESFORCE.SYNCQ`** neexistuje, most nebude pokračovat bez ohledu na kvalitu režimu služby. Skript MQSC je poskytnut pro vytvoření fronty s relevantními atributy. Fronta musí být konfigurována s volbou `DEFSOPT (EXCL) NOSHARE` , aby bylo zajištěno, že pouze jedna instance programu mostu může aktualizovat frontu **`SYSTEM.SALESFORCE.SYNCQ`** .

Chcete-li vytvořit konfiguraci pro vytváření zpráv událostí pro události platformy, prohlédněte si téma "Vytvoření zpráv událostí pro události platformy Salesforce" na stránce 774.

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 údaje a pověření zabezpečení Salesforce a certifikát podepsaný držitelem, přeskočte na krok “3” na stránce 769.

   Volitelné: Vytvořte token zabezpečení pro váš účet Salesforce .
   a) Přihlaste se ke svému účtu Salesforce .
   b) Vytvořte nebo obnovte token zabezpečení pomocí kroků uvedených v článku nápovědy Salesforce help: Reset vašeho tokenu zabezpečení.
3. V produktu Salesforcevytvořte bezpečnostní certifikát podepsaný CA.
   a) Vyberte volbu **Řízení zabezpečení** z nabídky **Spravovat** na stránce **Domovská stránka Force.com** a poté na volbu **Správa certifikátů a klíčů**.

      Otevře se stránka **Správa certifikátů a klíčů** .
   b) Klepněte na volbu **Vytvořit certifikát podepsaný CA**.

      Otevře se stránka **Certifikáty** .
   c) Do pole **Popisek** zadejte název certifikátu, stiskněte klávesu Taba poté klepněte na tlačítko **Uložit**.

      Zobrazí se informace o certifikátu a podrobnostech klíče.
   d) Klepněte na tlačítko **Zpět na seznam: Certifikáty a klíče**.
   e) Klepněte na volbu **Exportovat do úložiště klíčů**.
   f) Zadejte heslo pro úložiště klíčů a poté klepněte na tlačítko **Exportovat**.
   g) Uložte exportované úložiště klíčů do lokálního systému souborů.
4. Pomocí rozhraní GUI správy klíčů produktu IBM otevřete úložiště klíčů, které jste exportovali z produktu Salesforce , a naplňte certifikáty podepisujících subjektů.
   a) Spuštěním příkazu **strmqikm** otevřete grafické uživatelské rozhraní správy klíčů produktu IBM .

      Další informace naleznete v tématu Použití runmqckm, runmqakm a strmqikm pro správu digitálních certifikátů.
   b) Klepněte na volbu **Otevřít soubor databáze klíčů** a přejděte do umístění úložiště klíčů produktu Salesforce .
   c) Klepněte na tlačítko **Otevřít**, ujistěte se, že jste vybrali **JKS** z voleb **Typ databáze klíčů** , poté klepněte na tlačítko **OK**.
   d) Zadejte heslo, které jste vytvořili pro úložiště klíčů v kroku 3f, a poté klepněte na tlačítko **OK**.
   e) Vyberte volbu **Certifikáty podepsaného** z voleb **Obsah databáze klíčů** .
   f) Klepněte na **Naplnit**.
   g) Vyberte zaškrtávací políčko **Verisign Inc.** ze seznamu **Přidat certifikáty CA** a poté klepněte na tlačítko **OK**.
5. Volitelné: Vytvořte klíč spotřebitele OAuth a utajené údaje vytvořením připojení aplikace pro produkt IBM MQ Bridge to Salesforce ve vašem účtu Salesforce .

   Potřebujete kódy **Klíč spotřebitele** a **Utajený údaj spotřebitele** , používáte-li produkt IBM MQ Bridge to Salesforce v produkčních prostředích.
   a) Vyberte volbu **Vytvořit**, poté volbu **Aplikace** z nabídky **Sestavit** na stránce **Domovská stránka Force.com** .

      Otevře se stránka Aplikace.

b) Klepněte na volbu **Nový** v sekci **Připojené aplikace** .

Otevře se stránka **Nová připojená aplikace** .

c) Zadejte název pro IBM MQ Bridge to Salesforce do pole **Název připojené aplikace**, například **MQBridgeToSalesforce**.

d) Zadejte **Název rozhraní API**.

Pokud přejdeš na další pole, **Připojený název aplikace** se zkopíruje do pole názvu **Název rozhraní API** .

e) Zadejte **Kontaktní e-mail**.

f) Vyberte volbu **Povolit nastavení OAuth** v sekci **Rozhraní API (Enable OAuth Settings)** .

Další možnosti v této sekci jsou pak prezentovány.

g) Přidejte adresu **Adresa URL zpětného volání**, například `https://www.ibm.com`.

h) Vyberte volbu **Úplný přístup (plný)** ze seznamu **Dostupné rozsahy OAuth** v sekci **Vybrané rozsahy OAuth** a poté klepněte na tlačítko **Přidat**, chcete-li přidat úplný přístup do seznamu **Vybrané rozsahy OAuth** .

i) Klepněte na tlačítko **Uložit**.

j) Klepněte na tlačítko **Pokračovat**.

k) Poznamenejte si kódy **Klíč spotřebitele** a **Tajné údaje spotřebitele** .

6. Vytvořte požadovanou frontu synchronizace ve správci front.

```
cat /opt/mqm/mqsf/samp/mqsfbSyncQ.mqsc | runmqsc SQM1
```

Fronta synchronizace udržuje stav události po restartu aplikace nebo správce front. Hloubka fronty může být malá, protože ve frontě se očekává pouze jedna zpráva. V daném okamžiku může v daném okamžiku běžet pouze jedna instance mostu, takže jsou výchozí volby nastaveny pro výhradní přístup.

7. Vytvořte konfigurační soubor s parametry připojení a zabezpečení pro IBM MQ, Salesforcea chování IBM MQ Bridge to Salesforce .

```
runmqsfb -o new_config.cfg
```

Existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte tlačítko `Enter` , chcete-li přijmout existující hodnoty, stiskněte klávesu `Space` a pak `Enter` , čímž vymažete hodnoty, a pak zadejte `Enter` a přidejte nové hodnoty.

a) Zadejte hodnoty pro připojení ke správci front SQM1:

Minimální hodnoty, které jsou potřeba pro připojení, jsou název správce front, základní kořen tématu produktu 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 požadován, pokud se připojujete lokálně. Název správce front a základní téma v konfiguračním souboru nemusíte zadávat tak, jak je lze zahrnout do příkazového řádku později při spuštění mostu.

b) Zadejte hodnoty pro připojení k produktu Salesforce:

Minimální hodnoty, které jsou potřeba 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, které jsou potřeba pro připojení TLS, jsou cestou k úložišti klíčů pro certifikáty TLS a heslo úložiště klíčů. Není-li poskytnuta žádná cesta k důvěryhodnému úložišti nebo heslo, použijí se parametry úložiště klíčů a hesla pro důvěryhodné úložiště a heslo. Používáte-li TLS pro připojení ke správci front produktu 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 produktu IBM MQ Bridge to Salesforce:

Nemusíte měnit nebo poskytovat žádnou z těchto hodnot, ale znáte-li vaše téma nebo názvy událostí platformy, přidejte je sem. Mohou být také přidány později, v příkazovém řádku, když jste připraveni spustit most. Musíte určit 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 , která bude řídit provádění programu. Upravte ukázkový soubor `mqsfbService.mqsc` tak, aby ukazoval na nově vytvořený konfigurační soubor, a proveďte všechny další změny parametrů příkazu.

```
cat modified mqsfbService.mqsc | runmqsc SQM1
```

9. Volitelné: Postupujte podle pokynů v tématu Začínáme s produktem IBM MQ Console a nastavte produkt IBM MQ Console.

10. Volitelné: Konfigurujte IBM MQ Bridge to Salesforce tak, aby se spouštěl jako uživatel bez jména uživatele root.

Chcete-li být schopni spustit příkaz IBM MQ Bridge to Salesforce jako *bezspojku*, například v rámci *kontejneru bez kořenů*, musí být správně nastaveny adresáře Java `userRoot` a `systemRoot` , aby se zajistilo přístup pro čtení a 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 Salesforce témat a událostí platformy, a publikovat je do své sítě IBM MQ .

Jak pokračovat dále

Postupujte podle kroků pro produkt “Spuštění prostředí IBM MQ Bridge to Salesforce” na stránce 781.

Související úlohy

Trasování IBM MQ Bridge to Salesforce

Monitorování produktu IBM MQ Bridge to Salesforce

Související odkazy

runmqsfb (spuštění produktu IBM MQ Bridge na Salesforce)

V 9.1.2 Linux Další volby konfigurace pro IBM MQ Bridge to Salesforce

Produkt IBM MQ 9.1.2 zavádí další volby konfigurace, které povolují dvě hlavní třídy další topologie, které se zabývají "příchozí" (události generované z produktu Salesforce, jsou publikovány do aplikací produktu IBM MQ) a "outbound" (události publikování aplikací produktuIBM MQ , které byly odeslány do produktu Salesforce). Kromě toho je zde změna způsobu, jakým probíhá trasování a protokolování práce.

Změny z IBM MQ 9.1.0 IBM MQ Bridge to Salesforce

Standardně nejsou provedeny žádné změny chování z mostu IBM MQ 9.1.0 , kromě souboru protokolu, který se nyní začíná otáčet. Další informace viz “Rotační protokoly” na stránce 773.

Hlavní změna spočívá v tom, že správce front nyní podporuje více instancí mostu. Chcete-li tuto funkci povolit a zbývající části těchto dalších topologií, musíte provést některé ruční změny konfigurace.

Viz runmqfsb , kde získáte další informace o dalších volbách konfigurace a “Příklad výstupu konfigurace” na stránce 774 pro příklad revidovaných informací o konfiguraci.

Oddělené příchozí práce

Více instancí mostu může pracovat s příchozími prací z produktu Salesforce do produktu IBM MQ, ale tyto musí pracovat na nezávislých sadách témat a událostí typu push produktu Salesforce . Jinak by existovala možnost opakovaných událostí pozorovaných aplikacemi produktu IBM MQ , protože neexistuje žádný protokol křížového mostu, který by zastavil duplikaci událostí. Každá instance používá svou vlastní konfigurovatelnou synchronizační frontu pro zadržení procesu **ReplayId**.

To je pravděpodobně užitečné, když:

- Různá témata produktu Salesforce mají různé autorizace zabezpečení. Každá instance mostu má jinou sadu pověření pro přístup k produktu Salesforce.
- Máte obavy z toho, že pracovní zátěž přicházející z produktu Salesforce je příliš velká na to, aby se mohl zpracovat jeden most. Proto můžete uspořádat témata, která mají být rozdělena na "A-M" procházející jedním mostem, a "N-Z" skrze jiné.

Sdílená odchozí práce

Most podporuje více instancí pro podporu odchozí práce odesílané z produktu IBM MQ do produktu Salesforce. Dojde-li k selhání jedné instance mostu, může zpracování publikací pokračovat dalšími instancemi, které jsou přihlášeny ke stejným tématům v rámci stejného správce front.

Poznámka: Pro tuto volbu nejsou zapotřebí žádné změny v konfiguraci tématu produktu IBM MQ .

Tyto spolupracující instance musí být nastaveny tak, aby jedna z instancí zpracovávali příchozí práci z produktu Salesforce, protože tato instance musí mít výlučný přístup k frontě synchronizace.

To je pravděpodobně užitečné, pokud máte obavy z:

- Zátěž přicházející z produktu IBM MQ. Vzhledem k tomu, že požadavky na Salesforce jsou synchronní, nemůže most zpracovat novou práci, zatímco stále zpracovává jednu zprávu. Existence více spotřebitelů tuto situaci zmírňuje.
- Architektura dostupnosti. Nyní je například možné spustit více instancí v samostatných datových centrech s možností lepšího překonání selhání a možností zotavení z havárie. Běží jako klient produktu IBM MQ také odděluje most od umístění správce front.

Interakce trasování a ladění

Příznak ladění pokračuje v činnosti jako předtím. To znamená, že *-d1* poskytuje informace ladění mostu a *-d2* zapíná protokolování ladění pro předem požadované komponenty. Pokud jste však povolili trasování produktu IBM MQ při spuštění mostu, je automatické zapnutí vytváření sestav na úrovni *-d2* automaticky zapnuto.

Rotační protokoly

Výchozí chování pro soubor protokolu se změní, aby mělo tři soubory protokolu, každá o velikosti 2 MB. Tyto hodnoty můžete přepsat pomocí dalších vlastností konfigurace. Existující konfigurační atribut nebo parametr příkazového řádku pro soubor protokolu se vezme jako základní název pro protokoly, s přidáním indexu.

Pokud má nakonfigurovaný soubor protokolu:

- Chybí typ souboru, index je přidán na konec názvu souboru.

  Nastavení souboru protokolu na `abc`, výsledky v protokolech s názvem `abc.0`, `abc.1`a tak dále.
- Typ souboru, před typem souboru je vložen index.

  Nastavení souboru protokolu na `abc.log`, výsledky v protokolech s názvem `abc.0.log`, `abc.1.log`a tak dále.

Notes:

1. Vzhledem k tomu, že mosty mohou být spuštěny s libovolným oprávněním uživatele, není možné vynutit u protokolů konkrétní adresář, například `/var/mqm/qmgrs/<qm>/errors`.
2. Tytéž informace jsou i nadále zapisovány do proudů *stdout* a *stderr* .
3. Při každém opětovném otevření jednotlivého souboru protokolu se znovu vytisknou základní informace o konfiguraci. Informace budou vždy dostupné místo toho, aby byly tisknuty pouze jednou na začátku programu.

Zachování protokolů

V nových topologiích je pravděpodobnější, že bude existovat více instancí mostu spuštěných pro konkrétního správce front.

Aby nedošlo k interferencím mezi jednotlivými instancemi a nedošlo k přepsání předchozích spuštění mostu, most se nespustí, pokud již protokol `.0` existuje.

Potřebujete spouštěcí proceduru, která odstraní předchozí kopie protokolu před spuštěním mostu, nebo přidá něco jako časové razítko do názvu.

Související úlohy

“Konfigurace produktu IBM MQ pro použití s akcemi typu push platformy Salesforce a událostmi platformy” na stránce 766
Tyto informace použijte k nastavení zabezpečení a připojení k produktu Salesforce a vaší síti IBM MQ , a to konfigurací a následným spuštěním IBM MQ Bridge to Salesforce.

Související odkazy

runmqfsb

V 9.1.2 Linux Příklad výstupu konfigurace

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

V 9.1.0 Linux Vytvoření zpráv událostí pro události platformy Salesforce

Můžete nakonfigurovat produkt IBM MQ a zadat `IBM MQ Bridge to Salesforce parameters` k vytvoření konfiguračního souboru a použít most k vytvoření zpráv událostí pro události platformy Salesforce .

Než začnete

- Nainstalovali jste balík produktu **MQSeriesSFBridge** ve vaší instalaci produktu IBM MQ na platformu x86-64 Linux .

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným k vytvoření konfiguračního souboru produktu IBM MQ Bridge to Salesforce a k úspěšnému připojení k produktu Salesforce a produktu IBM MQ , abyste mohli vytvářet zprávy událostí pro události platformy Salesforce . Další informace o významu a volbách pro všechny parametry naleznete v popisu příkazu runmqsfb . Musíte zvážit své vlastní požadavky na zabezpečení a přizpůsobit parametry vhodné pro vaši implementaci.

Chcete-li vytvořit konfiguraci pro přihlášení k odběru témat a událostí platformy, prohlédněte si téma “Konfigurace IBM MQ Bridge to Salesforce” na stránce 767.

Vytvoření zpráv událostí pro události platformy Salesforce

K vytvoření zpráv vložených do tématu správce front `/root/mqtosfb/event/+`můžete použít aplikaci IBM MQ . Most se přihlásí k odběru daného tématu, získá obsah ze zpráv a použije jej k publikování zpráv událostí pro událost platformy Salesforce . Další informace o událostech platformy naleznete v tématu Dodání vlastních oznámení s událostmi platformy v dokumentaci vývojáře Salesforce .

Chcete-li povolit vytváření zpráv událostí pomocí mostu, je třeba poskytnout dva atributy, které jsou dodatkem k těm, které se používají k přihlášení k odběru témat a událostí platformy:

- Vytvořte a přidejte název serveru **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 bridge**.

Musíte vytvořit událost platformy v produktu Salesforce a definovat pole obsahu předtím, než budete moci použít tento most k vytvoření zpráv událostí pro danou událost platformy. Název události platformy a její obsah určují, jak budete potřebovat formátovat zprávu IBM MQ , která je zpracována mostem. Například, pokud vaše událost platformy Salesforce **Object name** je *MQPlatformEvent1* a vaše dvě uživatelsky definovaná pole jsou textová pole s **API name** *MyText__c* a *Name__c*, pak vaše zpráva IBM MQ , která je publikována na `/root/mqtosfb/event/MQPlatformEvent1__e` , musí být správně naformátovaná JSON, jak je uvedeno níže:

```
{ "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 formátované zprávy MQFMT_STRING.

Pokud již máte událost platformy, pro kterou chcete vytvořit zprávy událostí, prohlédněte si krok “7” na stránce 777 , abyste vytvořili událost platformy v produktu Salesforce , nebo tento krok přeskočte. Musíte naformátovat zprávu IBM MQ tak, aby odpovídala polím, která jsou nastavena ve vaší události platformy Salesforce . Pole v rámci události platformy Salesforce mohou být označena jako volitelná nebo povinná. Další informace naleznete v části Pole událostí platformy v dokumentaci vývojáře produktu Salesforce .

Je-li most spuštěn, přihlašuje se k odběru určeného tématu IBM MQ .

- Určíte-li v konfiguraci mostu kvalitu služby produktu **At-most-once** , bude odběr, který most vytvoří, netrvalý. Všechny publikace, které jsou prováděny aplikacemi produktu IBM MQ v době, kdy most není spuštěn, nebudou zpracovány.
- Určíte-li kvalitu služby produktu **At-least-once** v konfiguraci mostu, bude odběr z daného mostu trvalý. To znamená, že most může zpracovávat publikování, která jsou prováděna aplikacemi produktu IBM MQ v době, kdy není spuštěn most. Trvalé odběry vyžadují známý odběr a ID klienta. Most používá jako název odběru *D_SUB_RUNMQSFB* jako název odběru a *runmqsfb_1* jako ID klienta.

Je-li most použit k přihlášení k odběru Salesforce témat a událostí platformy a nikoli vytváření zpráv událostí, pokusí se odstranit trvalý odběr v případě, že dojde ke změně konfigurace, a odběr je nyní osiřelý.

Můžete odebrat trvalé odběry, které most vytváří takto:

Použijte IBM MQ Explorer.
Otevřete **složku odběrů** pro správce front, který most používá, a vyhledejte název odběru, který končí v souboru *:D_SUB_RUNMQSFB* , kde řetězec tématu je `/sf/mqtosfb/event+`. Klepněte pravým tlačítkem myši na název odběru a klepněte na volbu Odstranit. Dojde-li k chybě, která označuje, že odběr je používán, může být váš most stále spuštěn. Zastavte most a pokuste se odstranit odběr znovu.

K vyhledání a odstranění odběru použijte produkt `runmqsc` .
Spusťte rozhraní **`runmqsc`** a spusťte příkaz `DISPLAY SUB (*)`. Hledejte název odběru **SUB** končící v *:D_SUB_RUNMQSFB*. Zadejte dílčí příkaz delete a zahrňte soubor **SUBID** odběru, který chcete odstranit. Například `DELETE SUB SUBID(414D5120514D312020202020202020205C589459987E8620)`

Zastavte, poté spusťte most se službou `At-most-once` kvality služby.
Pokud jste spustili most s kvalitou služby **`At-least-once`** produktu `At-least-once delivery? (Y/N) :[Y]`, vytvoří se odběr, který je vytvořen. Chcete-li odstranit odběr, změňte kvalitu služby na `At-least-once delivery? (Y/N) :[N]` ve svém konfiguračním souboru a znovu spusťte most. Trvalý odběr je odstraněn a je vytvořen netrvalý 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 údaje a pověření zabezpečení Salesforce a certifikát podepsaný držitelem, přeskočte na krok 4.

   Volitelné: Vytvořte token zabezpečení pro váš účet Salesforce .
   a) Přihlaste se ke svému účtu Salesforce .
   b) Vytvořte nebo obnovte token zabezpečení pomocí kroků uvedených v článku nápovědy Salesforce help: Reset vašeho tokenu zabezpečení.
3. Vytvořte certifikát zabezpečení podepsaný sám sebou v produktu Salesforce.
   a) Vyberte volbu **Řízení zabezpečení** z nabídky **Spravovat** na stránce **Domovská stránka Force.com** a poté na volbu **Správa certifikátů a klíčů**.
   Otevře se stránka **Správa certifikátů a klíčů** .
   b) Klepněte na volbu **Vytvořit certifikát podepsaný svým držitelem**.
   Otevře se stránka **Certifikáty** .
   c) Do pole **Popisek** zadejte název certifikátu, stiskněte klávesu Taba poté klepněte na tlačítko **Uložit**.
   Zobrazí se informace o certifikátu a podrobnostech klíče.
   d) Klepněte na tlačítko **Zpět na seznam: Certifikáty a klíče**.
   e) Klepněte na volbu **Exportovat do úložiště klíčů**.
   f) Zadejte heslo pro úložiště klíčů a poté klepněte na tlačítko **Exportovat**.
   g) Uložte exportované úložiště klíčů do lokálního systému souborů.
4. Pomocí rozhraní GUI správy klíčů produktu IBM otevřete úložiště klíčů, které jste exportovali z produktu Salesforce , a naplňte certifikáty podepisujících subjektů.

a) Spuštěním příkazu **strmqikm** otevřete grafické uživatelské rozhraní správy klíčů produktu IBM . Další informace naleznete v tématu Použití runmqckm, runmqakm a strmqikm pro správu digitálních certifikátů.

b) Klepněte na volbu **Otevřít soubor databáze klíčů** a přejděte do umístění úložiště klíčů produktu Salesforce .

c) Klepněte na tlačítko **Otevřít**, ujistěte se, že jste vybrali **JKS** z voleb **Typ databáze klíčů** , poté klepněte na tlačítko **OK**.

d) Zadejte heslo, které jste vytvořili pro úložiště klíčů v kroku 3f, a poté klepněte na tlačítko **OK**.

e) Vyberte volbu **Certifikáty podepsaného** z voleb **Obsah databáze klíčů** .

f) Klepněte na **Naplnit**.

g) Vyberte zaškrtávací políčko **Verisign Inc.** ze seznamu **Přidat certifikáty CA** a poté klepněte na tlačítko **OK**.

5. Volitelné: Vytvořte klíč spotřebitele OAuth a utajené údaje vytvořením připojení aplikace pro produkt IBM MQ Bridge to Salesforce ve vašem účtu Salesforce .

   Potřebujete kódy **Klíč spotřebitele** a **Utajený údaj spotřebitele** , používáte-li produkt IBM MQ Bridge to Salesforce v produkčních prostředích.

   a) Vyberte volbu **Vytvořit**, poté volbu **Aplikace** z nabídky **Sestavit** na stránce **Domovská stránka Force.com** .

      Otevře se stránka **Aplikace** .

   b) Klepněte na volbu **Nový** v sekci **Připojené aplikace** .

      Otevře se stránka **Nová připojená aplikace** .

   c) Zadejte název pro IBM MQ Bridge to Salesforce do pole **Název připojené aplikace**, například **MQBridgeToSalesforce**.

   d) Zadejte **Název rozhraní API**.

      Pokud přejdeš na další pole, **Připojený název aplikace** se zkopíruje do pole názvu **Název rozhraní API** .

   e) Zadejte **Kontaktní e-mail**.

   f) Vyberte volbu **Povolit nastavení OAuth** v sekci **Rozhraní API (Enable OAuth Settings)** .

      Další možnosti v této sekci jsou pak prezentovány.

   g) Přidejte adresu **Adresa URL zpětného volání**, například `https://www.ibm.com`.

   h) Vyberte volbu **Úplný přístup (plný)** ze seznamu **Dostupné rozsahy OAuth** v sekci **Vybrané rozsahy OAuth** a poté klepněte na tlačítko **Přidat**, chcete-li přidat úplný přístup do seznamu **Vybrané rozsahy OAuth** .

   i) Klepněte na tlačítko **Uložit**.

   j) Klepněte na tlačítko **Pokračovat**.

   k) Poznamenejte si kódy **Klíč spotřebitele** a **Tajné údaje spotřebitele** .

6. Vytvořte požadovanou synchronizaci a chybové fronty ve správci front.

   ```
   cat /opt/mqm/mqsf/samp/mqsfbSyncQ.mqsc | runmqsc PEQM1
   ```

   Fronta synchronizace udržuje stav události po restartu aplikace nebo správce front. Hloubka fronty může být malá, protože ve frontě se očekává pouze jedna zpráva. V daném okamžiku může v daném okamžiku běžet pouze jedna instance mostu, takže jsou výchozí volby nastaveny pro výhradní přístup. Než budete moci použít most k vytvoření zpráv událostí pro události platformy, musí být vytvořena fronta chyb. Fronta chyb se používá pro zprávy, které nemohou být úspěšně zpracovány produktem Salesforce. Musíte přidat název fronty chyb v sekci konfiguračního parametru mostu **Connection to Queue Manager** , jak je zobrazeno v kroku “8.a” na stránce 778.

7. Volitelné: Vytvořte objekt události platformy na svém účtu Salesforce .

a) Vyberte položku **Události platformy** v nabídce **Vývoj** na stránce **Force.com Home** a poté klepněte na volbu **Nová událost platformy**.

Otevře se stránka **Nová událost platformy** .

b) Vyplňte pole **Popisek** a **Štítek plural** .

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 délky polí **Typ dat** na hodnotu *Text (64)* a *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 produktu IBM MQ , do kterého můžete vložit zprávy, které má most zpracovávat. Například, můžete použít ukázku **AMQSPUBA** k přidání následující formátované zprávy JSON do tématu `/sf/mqtosfb/event/`*`Salesforce Platform Object Name/API name`* :

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

Můžete spustit ukázku produktu **AMQSPUBA** a vytvořit zprávy po spuštění mostu. V adresáři *MQ `installation location`*`/samp/bin` zadejte následující příkaz:

```
./amqspub /sf/mqtosfb/event/Salesforce Platform Object Name/API name PEQM1
```

Na výzvu k zadání zadejte zprávu ve formátu JSON.

8. Vytvořte konfigurační soubor s parametry připojení a zabezpečení pro IBM MQ, Salesforcea chování IBM MQ Bridge to Salesforce .

```
runmqsfb -o new_config.cfg
```

Existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte tlačítko `Enter` , chcete-li přijmout existující hodnoty, stiskněte klávesu `Space` a pak `Enter` , čímž vymažete hodnoty, a pak zadejte `Enter` a přidejte nové hodnoty.

a) Zadejte hodnoty pro připojení ke správci front PEQM1:

Minimální hodnoty, které jsou potřeba pro připojení, jsou název správce front, základní kořen tématu produktu 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, jméno kanálu není povinné. Název správce front a základní téma v konfiguračním souboru nemusíte zadávat tak, jak je lze zahrnout do příkazového řádku později při spuštění mostu.

b) Zadejte hodnoty pro připojení k produktu Salesforce:

Minimální hodnoty, které jsou potřeba 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, které jsou potřeba pro připojení TLS, jsou cestou k úložišti klíčů pro certifikáty TLS a heslo úložiště klíčů. Není-li poskytnuta žádná cesta k důvěryhodnému úložišti nebo heslo, použijí se parametry úložiště klíčů a hesla pro důvěryhodné úložiště a heslo. Používáte-li TLS pro připojení ke správci front produktu 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 produktu IBM MQ Bridge to Salesforce:

Musíte změnit volbu **Subscribe to MQ publications for platform events** z výchozí hodnoty *N*na *Y* , abyste mohli použít most k vytvoření zpráv událostí. 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 , která bude řídit provádění programu. Upravte ukázkový soubor `mqsfbService.mqsc` tak, aby ukazoval na nově vytvořený konfigurační soubor, a proveďte všechny další změny parametrů příkazu.

```
cat modified mqsfbService.mqsc | runmqsc PEQM1
```

10. Volitelné: Postupujte podle pokynů v tématu Začínáme s produktem IBM MQ Console a nastavte produkt IBM MQ Console.
11. Volitelné: Přidejte a nakonfigurujte moduly widget ve své instanci produktu IBM MQ Console , abyste zobrazili data produktu Salesforce .
    a) Klepněte na volbu **Přidat modul widget**.

    Otevře se nový modul widget.

    b) Vyberte **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 Bridge** .

    f) Z rozevírací nabídky **Třída prostředků**vyberte volbu **Stav mostu**.

    g) Vyberte volbu **MQ-vytvořené události platformy**, z rozevírací nabídky **Typ prostředku**.

    h) Vyberte volbu **Celkem MQ-vytvořené události platformy**z rozevírací nabídky **Prvek prostředku**.

    i) Klepněte na tlačítko **Uložit**.

    Nakonfigurovali jste produkt IBM MQ Console pro zobrazení celkového počtu událostí platformy IBM MQ vytvořených platformou. Když je spuštěn most a vy začnete vkládat zprávy do tématu `/sf/mqtosfb/event/`*`Salesforce Platform Object Name/API name`* , modul widget zobrazí celkový počet událostí zpráv, které most vytvořil.

V 9.1.0 Formát zprávy a chybové zprávy pro IBM MQ Bridge to Salesforce

Informace o formátování zpráv, které zpracovává IBM MQ Bridge to Salesforce.

Aplikace vloží zprávu do specifického tématu správce front, například /*root*/mqtosfb/event/MQPlatformEvent1__e. Most se přihlásí k odběru daného tématu, získá obsah ze zpráv a použije jej k publikování zpráv událostí pro událost platformy Salesforce .

Musíte vytvořit událost platformy v produktu Salesforce a definovat pole obsahu předtím, než budete moci použít tento most k vytvoření zpráv událostí pro danou událost platformy. Název události platformy a její obsah určují, jak budete potřebovat formátovat zprávu IBM MQ , která je zpracována mostem. Například, pokud vaše událost platformy Salesforce **Object name** je *MQPlatformEvent1* a vaše dvě uživatelsky definovaná pole jsou textová pole s **API name** *MyText__c* a *Name__c*, pak vaše zpráva IBM MQ , která je publikována na /*root*/mqtosfb/event/MQPlatformEvent1__e , musí být správně naformátovaná JSON, jak je uvedeno níže:

```
{ "MyText__c" : "Some text here", "Name__c" : "Bob Smith" }
```

Zprávy, které jsou spotřebovávány a produkovány mostem, jsou textové zprávy (MQSTR) ve formátu JSON. Vstupní zpráva je jednoduchý JSON a programy mohou použít zřetězení řetězce, aby jej vygenerovaly.

Chybové zprávy

Chyby mohou být zjištěny přemostění, například pokud zpráva není v textovém formátu nebo Salesforce, například pokud název události platformy neexistuje. Pokud se při zpracování vstupní zprávy vyskytne chyba, zpráva se přesune do fronty chyb mostu spolu s vlastnostmi, které popisují chybu. Chyba je také zapsána do proudu *stderr* pro most.

Chyby, které jsou generovány 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"}
```

Špatný JSON, stav 400 textu

```
{"errorCode":"NOT_FOUND","message":"The requested resource does not exist"}
```

Zpráva není JSON, stav 400 text

```
[{"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"}
```

Není textová zpráva (neodeslána do Salesforce)

```
Error: Publication on topic ' /sf/mqtosfb/event/MQPlatformEvent1' does not contain a text
formatted message
```

V 9.1.0 Linux Spuštění prostředí IBM MQ Bridge to Salesforce

Spuštěním příkazu IBM MQ Bridge to Salesforce se připojíte k produktu Salesforce a IBM MQ. Po připojení může most vytvořit odběry témat Salesforce a znovu publikovat zprávy na téma IBM MQ . Most může také vytvořit zprávy událostí pro události platformy Salesforce .

Než začnete

V úloze jste dokončili kroky konfigurace:

- “Konfigurace IBM MQ Bridge to Salesforce” na stránce 767
- “Vytvoření zpráv událostí pro události platformy Salesforce” na stránce 774

.

Informace o této úloze

Použijte konfigurační soubor, který jste vytvořili v předchozí úloze, ke spuštění produktu IBM MQ Bridge to Salesforce. Pokud jste nezahrnuli všechny požadované parametry do svého konfiguračního souboru, ujistěte se, že jste je zahrnuli do příkazového řádku.

Postup

1. Definujte vložit témata nebo události platformy v produktu Salesforce , které chcete přihlásit k odběru nebo události platformy, pro které chcete vytvořit zprávy událostí.
2. Spusťte produkt IBM MQ Bridge to Salesforce a připojte se k produktu Salesforce a vašemu správci front. Pokud spouštíte most pro přihlášení k odběru událostí produktu Salesforce , začleňte název typu push nebo platformy platformy, které jste definovali v kroku 1.

   ```
   runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName
   ```

   Je-li most připojen, jsou vráceny následující zprávy:

   - Pokud používáte most k přihlášení k odběru témat typu push platformy Salesforce a událostí platformy:

     ```
     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.
     ```

   - Používáte-li most k vytvoření 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 produktu Salesforce , pokud jsou zprávy vrácené po spuštění mostu označeny, že připojení nebylo úspěšné.
   a) Vydejte příkaz v režimu ladění s volbou ladění 1.

      ```
      runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName -d 1
      ```

      Kroky mostu jsou přes připojení nastavené a zobrazují zprávy o zpracování v režimu terse.

   b) Vydejte příkaz v režimu ladění s volbou ladění 2.

      ```
      runmqsfb -f new_config.cfg -r logFile -p PushtopicName -e eventName -d 2
      ```

      Pomocí tohoto příkazu lze procházet kroky mostu a zobrazovat zprávy zpracování v režimu s komentářem. Úplný výstup je zapsán do vašeho souboru protokolu.
4. Generujte události pomocí rozhraní produktu Salesforce k úpravě záznamů v databázi.

5. Přejděte na IBM MQ Console , kde uvidíte změny k odeslání témat v modulu widget, který jste nakonfigurovali v předchozí úloze.

Jak pokračovat dále

Použijte proměnnou *MQSFB_EXTRA_JAVA_OPTIONS* k předání ve vlastnostech prostředí JVM, například pro povolení trasování IBM MQ . Další informace najdete v tématu Trasování produktu IBM MQ Bridge to Salesforce.

Související úlohy

Monitorování produktu IBM MQ Bridge to Salesforce

Související odkazy

runmqsfb (spuštění produktu IBM MQ Bridge na Salesforce)

V 9.1.0 z/OS MQ Adv. Linux Konfigurace produktu IBM MQ pro použití s blockchain

Nastavte a spusťte program IBM MQ Bridge to blockchain tak, aby bezpečně připojil správce front Linux IBM MQ Advanced nebo z/OS IBM MQ Advanced for z/OS Value Unit Edition a IBM Blockchain. Prostřednictvím mostu lze asynchronně připojit, vyhledat a aktualizovat stav prostředku ve vašem řetězci blockchain pomocí aplikace systému zpráv, která se připojuje ke správci front IBM MQ Advanced nebo IBM MQ Advanced for z/OS VUE .

Než začnete

Poznámka: Produkt IBM MQ Bridge to blockchain je zamítnutý ve všech vydáních z 22. listopadu 2022 (viz Oznamovací dopis USA 222-431).

Upozornění: V 9.1.4 Produkt IBM MQ Bridge to blockchain postavený na systému Hyperledger Composer již není podporován.

Chcete-li používat produkt IBM MQ Bridge to blockchain postavený v produktu Hyperledger Fabric, musíte být spuštěn s produktem IBM MQ 9.1.4 .

- Produkt IBM MQ Bridge to blockchain je k dispozici pro připojení k:
  - Linux IBM MQ Advancednebo
  - z/OS IBM MQ Advanced for z/OS VUE

  jsou pouze správci front.
- V 9.1.4 Správce front musí být na stejné úrovni příkazů jako most, nebo vyšší, například 9.1.4.
- V 9.1.4 IBM MQ Bridge to blockchain je podporováno pro použití se svou sítí blockchain, která je založena na architektuře Hyperledger Fabric 1.4 .

Informace o této úloze

Blockchain je sdílená, distribuovaná digitální kniha, která se skládá z řetězce bloků, které představují odsouhlasené transakce mezi objekty typu peer v síti. Každý blok v řetězci je propojen s předchozím blokem atd. zpět k první transakci.

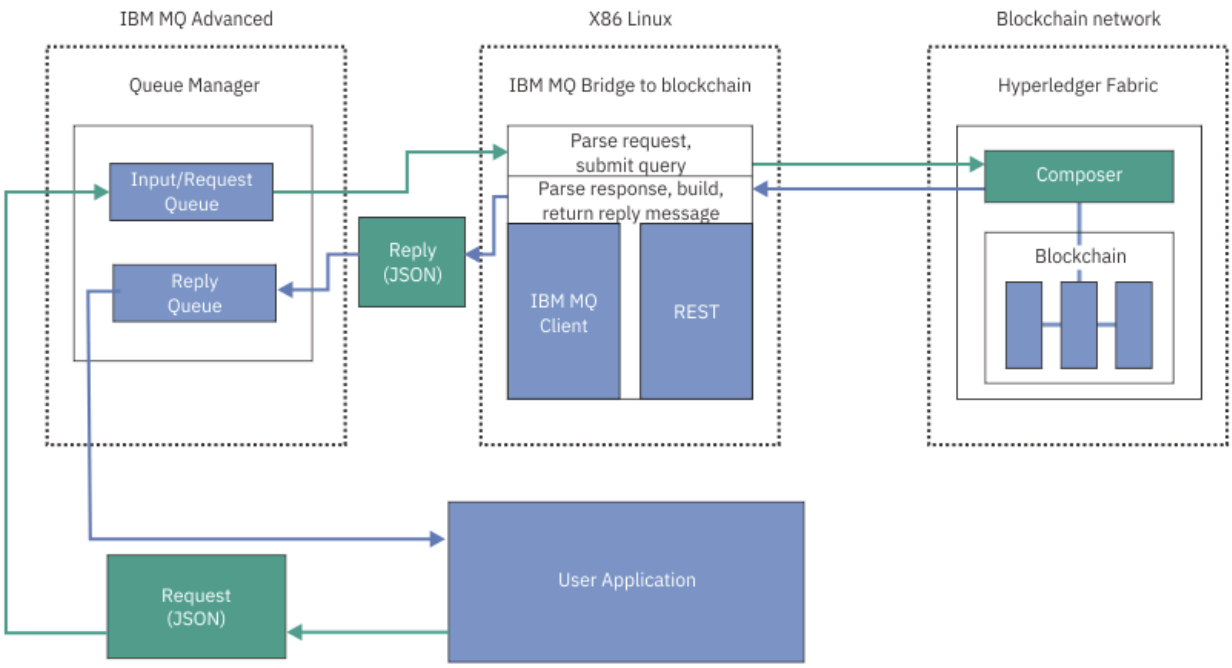
Produkt IBM Blockchain je postaven na produktu Hyperledger Fabric a můžete s ním pracovat lokálně pomocí produktu Docker nebo v kontejneru kontejneru v produktu IBM Cloud (formerly Bluemix). Můžete také aktivovat a používat svou síť IBM Blockchain ve výrobě, vytvářet a spravovat obchodní síť s vysokou úrovní zabezpečení, soukromí a výkonu. Další informace naleznete v příručce IBM Blockchain Platform.

Hyperledger Fabric je open source, podnikový blockchain framework, který je vyvíjen ve spolupráci s členy Hyperledger Project, včetně IBM jako výchozího přispěvatele kódu. Hyperledger Project,

nebo Hyperledgerje Linux Foundation open source, global, collaborative initiative to advance cross-industry blockchain technologies. Další informace naleznete v tématu IBM Blockchain, Projekty produktuHyperledgera Hyperledger Fabric.

Pokud již používáte produkt IBM MQ Advancednebo IBM MQ Advanced for z/OS VUEa IBM Blockchain, můžete pomocí konzoly IBM MQ Bridge to blockchain odesílat jednoduché dotazy, aktualizace a přijímat odpovědi ze sítě blockchain. Tímto způsobem můžete integrovat svůj místní software IBM se službou blockchain cloudu.

Stručný přehled operačního procesu mostu je zobrazen na obrázku 1. Uživatelská aplikace vloží do fronty vstupu/požadavku ve správci front IBM MQ Advancednebo IBM MQ Advanced for z/OS VUE zformátovanou zprávu ve formátu JSON. Most se připojí ke správci front, získá zprávu ze vstupní/fronty požadavků, zkontroluje, zda je JSON správně naformátovaný, a pak vydá dotaz nebo aktualizaci řetězce blockchain. Data vrácená blockchasem je analyzována mostem a umístěna do fronty odpovědí, jak je definováno v původní zprávě požadavku IBM MQ . Uživatelská aplikace se může připojit ke správci front, získat zprávu odpovědi z fronty odpovědí a použít tyto informace.



Obrázek 98. IBM MQ Bridge to blockchain

Produkt IBM MQ Bridge to blockchain můžete nakonfigurovat tak, aby se připojoval k síti blockchain jako účastník nebo rovnocenný partner. Je-li most spuštěn, požaduje aplikace systému zpráv most k řízení rutin řetězových kódů, které se dotazují nebo aktualizují stav prostředku a vrátí výsledky jako odezvu do aplikace systému zpráv.

Postup

1. Vytvořte a spusťte správce front nebo spusťte existujícího správce front, který chcete použít spolu s 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 následující fronty, jsou k dispozici ukázkové definice front mostu:

- Pověření uživatele, například SYSTEM.BLOCKCHAIN.IDENTITY.QUEUE
- Vstup zprávy na most, například APPL1.BLOCKCHAIN.INPUT.QUEUE
- Odpovědi z řetězce blockchain, 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 uvést více front odpovědí, jednu pro každou z vašich aplikací. Není nutné používat definované fronty odpovědí. Chcete-li používat dynamické fronty pro odpovědi, musíte zvážit jejich konfiguraci zabezpečení.

Výsledky

Vytvořili jste fronty, které most vyžaduje ke zpracování zpráv z produktu IBM MQ a ze sítě blockchain.

Jak pokračovat dále

Use your IBM MQ Advanced, or IBM MQ Advanced for z/OS VUE, queue manager information and the credentials from your blockchain network to create a configuration file for the IBM MQ Bridge to blockchain.

V 9.1.0 Vytvoření konfiguračního souboru pro IBM MQ Bridge to blockchain

Zadejte správce front a parametry sítě blockchain, chcete-li vytvořit konfigurační soubor pro produkt 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 blockchainve svém prostředí x86 Linux .
- Byl spuštěn správce front produktu IBM MQ Advanced .

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným k vytvoření konfiguračního souboru produktu IBM MQ Bridge to blockchain a k úspěšnému připojení k sítím IBM Blockchain a IBM MQ .

Most je možné použít k připojení k sítím blockchain, které jsou založeny na produktu Hyperledger Fabric 1.4 architecture. Chcete-li použít most, potřebujete informace o konfiguraci ze sítě blockchain. V každém kroku v této úloze můžete najít příklad podrobností konfigurace, které jsou založeny na dvou různých konfigurovaných sítích blockchain:

- Hyperledger Fabric sítě, která běží v produktu Docker. Další informace naleznete v tématu Začínáme s produktem Hyperledger Fabric, Psaní vaší první aplikacea “Příklad souboru pověření sítě Hyperledger Fabric” na stránce 786.
- Síť Hyperledger Fabric , která se spouští v klastru Kubernetes v produktu IBM Cloud (formerly Bluemix). Další informace viz Vývoj v pískovišti cloudu na platformě IBM Blockchain Platform.

Další informace o významu a volbách pro všechny parametry obslužného programu IBM MQ Bridge to blockchain naleznete v popisu příkazu runmqbcb . Musíte zvážit své vlastní požadavky na zabezpečení a přizpůsobit parametry vhodné pro vaši implementaci.

Postup

1. Spusťte most a vytvořte konfigurační soubor.

   Potřebujete parametry ze souboru pověření sítě blockchain a ze správce front produktu IBM MQ Advanced .

   ```
   runmqbcb -o config_file_name.cfg
   ```

   Jak ukazuje následující příklad, existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte tlačítko `Enter` , chcete-li přijmout existující hodnoty, stiskněte `Space` a pak `Enter` , abyste vymazali hodnoty, a zapište do hranatých závorek a pak stiskněte klávesu `Enter` pro přidání nových hodnot. Můžete oddělit seznamy hodnot (např. rovnocenných uzlů) čárkami nebo každou hodnotu na novém řádku. Prázdný řádek ukončí seznam.

   Poznámka: Existující hodnoty nelze upravovat. Můžete je zachovat, nahradit nebo vymazat.

2. Zadejte hodnoty pro připojení ke správci front produktu IBM MQ Advanced .

   Minimální hodnoty, které jsou potřeba pro připojení, jsou názvy správce front, názvy vstupních a výstupních front mostu, které jste nadefinovali. Pro připojení ke vzdáleným správcům front také potřebujete **`MQ Channel`** a **`MQ Conname`** (hostitelská adresa a port, kde je spuštěn správce front). Chcete-li používat TLS pro připojení k produktu IBM MQ v kroku “4” na stránce 785, musíte použít rozhraní JNDI nebo tabulky CCDT a v souladu s tím uvést **`MQ CCDT URL`** nebo **`JNDI implementation class`** a **`JNDI provider URL`** .

   ```
   Connection to Queue Manager
   ---------------------------
   Queue Manager                      : [adv_qmgr_name]
   Bridge Input Queue                 : [APPL1.BLOCKCHAIN.INPUT.QUEUE]
   Bridge User Identity Queue         : [SYSTEM.BLOCKCHAIN.IDENTITY.QUEUE]
   MQ Channel                         : []
   MQ Conname                         : []
   MQ CCDT URL                        : []
   JNDI implementation class          :
     [com.sun.jndi.fscontext.RefFSContextFactory]
   JNDI provider URL                  : []
   MQ Userid                          : []
   MQ Password                        : []
   ```

3. 13. Zadejte pověření serveru Hyperledger Fabric pro vaši síť.

   Příklady toho, co byste měli očekávat, jsou zobrazeny 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 nemáte žádné.

   ```
   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.

   ```
   Behaviour 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 Peers, Orderers a certifikační autority. Tyto informace jsou však nyní uloženy v *konfiguračním souboru sítě*, který je propojen v sekci serveru Hyperledger Fabric v nastavení serveru.

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

Postupujte podle kroků pro produkt “Spuštění prostředí IBM MQ Bridge to blockchain” na stránce 788.

V 9.1.4 Příklad souboru pověření sítě Hyperledger Fabric

Obsah souboru `.yml` z lokálně převedeného systému Hyperledger Fabric blockchateb spuštěného v produktu Docker, který můžete použít ke konfiguraci produktu IBM MQ Bridge to blockchain.

Produkt IBM MQ Bridge to blockchain je k dispozici pro připojení k:

- Linux IBM MQ Advancednebo
- z/OS IBM MQ Advanced for z/OS VUE

jsou pouze správci front.

Poté, co jste propracovali výukové programy Začínáme s produktem Hyperledger Fabric , porozuměli Co se děje v zákulisía spustili vaši síť pomocí jednoho z ukázek Hyperledger Fabric, měli byste mít ve složce `/blockchain/fabric-samples/basic-network` následující konfigurační soubor.

Chcete-li se připojit k vaší síti blockchain, musíte použít podrobnosti konfigurace z tohoto souboru, jste-li “Vytvoření konfiguračního souboru pro IBM MQ Bridge to blockchain” na stránce 784.

```
{
  "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"
        }
      ]
    }
  }
}
```

V 9.1.0 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" na stránce 792 .
- 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.

V 9.1.0 z/OS Formáty zpráv pro IBM MQ Bridge to blockchain před IBM MQ 9.1.4

Informace o formátování zpráv, které jsou odesílány a přijímány produktem IBM MQ Bridge to blockchain.

LTS

Upozornění: Existující formát pro formáty zpráv je zastaralý. From IBM MQ 9.1.4, if you have a Hyperledger Fabric network, use the format of the messages described in "Formáty zpráv pro IBM MQ Bridge to blockchain z IBM MQ 9.1.4" na stránce 790.

Aplikace požaduje, aby IBM MQ Bridge to blockchain řídil Hyperledger Composer definované rozhraní API REST tak, aby postupovali na informace, které jsou drženy na řetězci blockchain. Aplikace to provede umístěním zprávy s požadavkem do fronty požadavků mostu. Výsledky požadavku REST jsou formátovány podle mostu 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 požadavku obsahují tři atributy:

metoda
Příkazové slovo REST použité pro volání rozhraní REST API produktu Hyperledger Composer , jako např. POST, DELETE nebo GET

path
Cesta k rozhraní REST API produktu Hyperledger Composer . Tato hodnota je přidána k základní adrese URL serveru. Cesta by měla začínat řetězcem "`api/`".

tělo
Obsah specifický pro danou metodu. To je často struktura JSON.

Následující příklad používá metodu POST k cestě `api/Traderk` vytvoření nového objektu Truder. Tělo uvádí třídu Traders, jak je definováno modelem Hyperledger Composer uživatele, a také uvádí další hodnoty potřebné k vytvoření nového Obchodního objektu v síti blockchain.

```
{ "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 nastavené na ID zprávy příchozí zprávy. Libovolné uživatelem definované vlastnosti se zkopírují ze zprávy požadavku do zprávy odpovědi. ID uživatele v odpovědi je nastaveno na ID uživatele původce.

statusCode je stavový kód HTTP. Je-li chyba z IBM MQ nebo z mostu, pak se použije odpovídající **statusCode** .

statusType je řetězec, buď *SUCCESS* , nebo *FAILURE*.

Pro úspěšné požadavky obsahuje prvek "**data**" ve zprávě odpovědi odpověď z vyvolaného rozhraní REST API produktu Hyperledger Composer .

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 odezvy na chybu 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 selhal při zpracování serverem REST produktu Hyperledger Composer

```
{
   "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, a to buď při pohledu na řetězec **statusType** , nebo z existence datového pole. Pokud při zpracování vstupní zprávy došlo k chybě a most jej neodesílá do bloku blockchain, je hodnota vrácená z mostu hodnotou MQRC, obvykle **MQRC_FORMAT_ERROR**.

V 9.1.4 Linux Formáty zpráv pro IBM MQ Bridge to blockchain z IBM MQ 9.1.4

Informace o formátování zpráv, které jsou odesílány a přijímány produktem IBM MQ Bridge to blockchain.

Aplikace vyžaduje, aby server IBM MQ Bridge to blockchain řídil server Hyperledger Fabric , aby pracoval na informacích, které jsou uloženy v řetězci blockchain. Aplikace to provede umístěním zprávy s požadavkem do fronty požadavků mostu. Výsledky požadavku jsou formátovány podle mostu 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 a obsahují čtyři prvky.

Formát zprávy požadavku

Zprávy požadavků obsahují následující atributy:

Operace
String-case necitlivý

`submit` pro aktualizace nebo `evaluate` pro dotazy

síť
Řetězec-někdy známé jako `channel` v Hyperledger Fabric

Smlouva.
Řetězec-inteligentní smlouva nebo balík řetězového kódu, který má být vyvolán

argumenty
Pole-obvykle řetězce, ale některé prvky mohou být vnořenými objekty JSON.

Skutečné argumenty pro **`contract`**, včetně názvu metody.

Příklad:

```
{
  "operation" : "Evaluate",
  "network"   : "mychannel",
  "contract"  : "marbles0",
  "args"      : [ "readMarble" , "marble1" ]
}
```

Poznámka: Kromě zabezpečení těchto prvků a že zpráva je platná JSON, nebude provedeno žádné ověření platnosti obsahu mostu. Most spoléhá na to, že Hyperledger Fabric zpracovává požadavek nebo vrací chyby.

Formát zprávy odpovědi

Zprávy odpovědí mají své ID korelace nastavené na ID zprávy příchozí zprávy. Libovolné uživatelem definované vlastnosti se zkopírují ze zprávy požadavku do zprávy odpovědi. ID uživatele v odpovědi je nastaveno na ID uživatele původce.

`statusCode` je stavový kód HTTP. Je-li chyba z IBM MQ nebo z mostu, pak se použije odpovídající **`statusCode`** .

`statusType` je řetězec, buď *SUCCESS* , nebo *FAILURE*.

Pro úspěšné požadavky obsahuje prvek "**`data`**" ve zprávě odpovědi odpověď z vyvolaného rozhraní REST API produktu Hyperledger Composer .

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 odezvy na chybu 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 selhal při zpracování serverem REST produktu Hyperledger Composer

```
{
   "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, a to buď při pohledu na řetězec **statusType** , nebo z existence datového pole. Pokud při zpracování vstupní zprávy došlo k chybě a most jej neodesílá do bloku blockchain, je hodnota vrácená z mostu hodnotou MQRC, obvykle **MQRC_FORMAT_ERROR**.

V 9.1.0 z/OS Spuštění ukázky klienta IBM MQ Bridge to blockchain

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 k vašemu IBM MQ Advancednebo IBM MQ Advanced for z/OS VUE, správci front a 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 USS, kde jsou nainstalovány komponenty USS 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.

Linux V 9.1.2 Další volby konfigurace pro IBM MQ Bridge to blockchain

Produkt IBM MQ 9.1.2 zavádí změnu způsobu, jakým trasování a protokolování pracuje na serveru IBM MQ Bridge to blockchain.

Změny z IBM MQ 9.1.0 IBM MQ Bridge to blockchain

Standardně nejsou provedeny žádné změny chování z mostu IBM MQ 9.1.0 , kromě souboru protokolu, který se nyní začíná otáčet. Další informace viz “Rotační protokoly” na stránce 795.

Interakce trasování a ladění

Příznak ladění pokračuje v činnosti jako předtím. To znamená, že *-d1* poskytuje informace ladění mostu a *-d2* zapíná protokolování ladění pro předem požadované komponenty. Pokud jste však povolili trasování produktu IBM MQ při spuštění mostu, je automatické zapnutí vytváření sestav na úrovni *-d2* automaticky zapnuto.

Rotační protokoly

Výchozí chování pro soubor protokolu se změní, aby mělo tři soubory protokolu, každá o velikosti 2 MB. Tyto hodnoty můžete přepsat pomocí dalších vlastností konfigurace. Existující konfigurační atribut nebo parametr příkazového řádku pro soubor protokolu se vezme jako základní název pro protokoly, s přidáním indexu.

Pokud má nakonfigurovaný soubor protokolu:

- Chybí typ souboru, index je přidán na konec názvu souboru.

  Nastavení souboru protokolu na `abc`, výsledky v protokolech s názvem `abc.0`, `abc.1`a tak dále.
- Typ souboru, před typem souboru je vložen index.

  Nastavení souboru protokolu na `abc.log`, výsledky v protokolech s názvem `abc.0.log`, `abc.1.log`a tak dále.

Notes:

1. Vzhledem k tomu, že mosty mohou být spuštěny s libovolným oprávněním uživatele, není možné vynutit u protokolů konkrétní adresář, například `/var/mqm/qmgrs/<qm>/errors`.
2. Tytéž informace jsou i nadále zapisovány do proudů *stdout* a *stderr* .
3. Při každém opětovném otevření jednotlivého souboru protokolu se znovu vytisknou základní informace o konfiguraci. Informace budou vždy dostupné místo toho, aby byly tisknuty pouze jednou na začátku programu.

z/OS Konfigurace správců front v systému z/OS

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

Než začnete

Před konfigurací produktu IBM MQsi přečtěte informace o koncepcích produktu IBM MQ for z/OS v tématu Koncepce produktuIBM MQ for z/OS.

z/OS Přečtěte si informace o plánování prostředí produktu IBM MQ for z/OS v tématu Plánování prostředí IBM MQ v systému z/OS .

Informace o této úloze

Po instalaci produktu IBM MQje třeba provést řadu úloh, než jej budete moci zpřístupnit uživatelům.

Procedura

- Informace o tom, jak konfigurovat správce front v systému IBM MQ for z/OSnaleznete v následujících dílčích tématech.

Související pojmy

IBM MQ for z/OS koncepce

Související úlohy

“Vytvoření správců front na více platformách” 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 prostředky, které jsou k ní přidruženy, zejména fronty, které vlastní. Poskytuje aplikacím pro volání rozhraní MQI (Message Queuing Interface) volání příkazů a příkazy k vytvoření, úpravě, zobrazení a odstranění objektů IBM MQ .

Zabezpečení

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

“Konfigurace připojení mezi 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

z/OS Zadání příkazů

Související odkazy

z/OS Obslužné programy IBM MQ for z/OS

z/OS Příprava na přizpůsobení správců front v systému z/OS

Toto téma vám pomůže při přizpůsobování správců front s podrobnými informacemi o instalovatelných funkcích, národním jazykovým funkcím a informacím o testování a nastavení zabezpečení.

Příprava na přizpůsobení

Adresář programu uvádí obsah instalační pásky IBM MQ , informace o programu a servisní úrovni pro produkt IBM MQa popisuje, jak nainstalovat produkt IBM MQ for z/OS pomocí nástroje SMP/E (System Modification Program Extended). Program Directory for IBM MQ for z/OS lze stáhnout z adresáře IBM Centrum publikací (viz IBM MQ for z/OS Program Directory PDF files).

Pokud jste nainstalovali produkt IBM MQ, musíte provést řadu úloh, než jej budete moci zpřístupnit uživatelům. Popis těchto úloh najdete v následujících částech:

- “nastaveníIBM MQ for z/OS” na stránce 800
- “Testování správce front v systému z/OS” na stránce 863
- Nastavení zabezpečení v systému z/OS

Provádíte-li migraci z předchozí verze produktu IBM MQ for z/OS, není třeba provádět většinu úloh přizpůsobení. Další informace o úlohách, které musíte provést, viz Údržba a migrace .

Instalovatelné funkce produktu IBM MQ for z/OS

Produkt IBM MQ for z/OS se skládá z následujících funkcí:

Base
Tento požadavek je povinný; zahrnuje všechny hlavní funkce, včetně

- Administrace a obslužné programy
- Podpora aplikací CICS, IMSa dávkových typů pomocí rozhraní IBM MQ Application Programming Interface, nebo C++
- Distribuované zařízení řazení do front (podpora komunikace TCP/IP a APPC)

Funkce národního jazyka
Ty obsahují chybové zprávy a panely ve všech podporovaných národních jazycích. Každý jazyk má k sobě přidružený jazykový dopis. Jazyky a písmena jsou:

C
Zjednodušená čínština

E
U.S. angličtina (smíšená velikost písmen)

F
Francouzština

K
japonština

U

U.S. Angličtina (velká písmena)

Musíte nainstalovat volbu americké angličtiny (smíšená velikost písmen). Můžete také instalovat jeden nebo více jiných jazyků. (Proces instalace pro jiné jazyky vyžaduje instalaci americké angličtiny (smíšená velikost písmen), a to i v případě, že nechcete používat americkou angličtinu (smíšená velikost písmen).)

IBM MQ for z/OS Komponenty služeb systému Unix

Tato funkce je volitelná. Vyberte tuto funkci, chcete-li sestavit a spustit aplikace produktu Java , které používají produkt Java Message Service (JMS) pro připojení k produktu IBM MQ for z/OS nebo chcete-li sestavit a spustit aplikace HTTP, které používají protokol HTTP pro připojení k produktu IBM MQ for z/OS.

V 9.1.0 **IBM MQ for z/OS Systém Unix-Webové komponenty služeb systému**

Tato funkce je volitelná.

Vyberte tuto funkci, chcete-li použít IBM MQ Console, nebo REST API.

You must install the IBM MQ for z/OS Unix System Services Components feature, to install this feature.

Knihovny, které existují po instalaci

Produkt IBM MQ je dodáván s řadou samostatných zaváděcích knihoven. Tabulka 53 na stránce 797 zobrazuje knihovny, které mohou existovat až po instalaci produktu IBM MQ.

Tabulka 53. Knihovny produktu 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. Angličtina (smíšená velikost písmen) verze produktu IBM MQ.
thlqual.SCSQANLF	Obsahuje zaváděcí moduly pro francouzskou verzi produktu IBM MQ.
thlqual.SCSQANLK	Obsahuje zaváděcí moduly pro japonskou verzi produktu IBM MQ.
thlqual.SCSQANLU	Obsahuje zaváděcí moduly pro U.S. Anglická (velká) verze produktu IBM MQ.
thlqual.SCSQASMS	Obsahuje zdroj pro ukázkové programy asembleru.
thlqual.SCSQAUTH	Hlavní úložiště pro všechny moduly načtení produktu IBM MQ ; obsahuje také výchozí modul parametrů CSQZPARM. Tato knihovna musí být autorizovaná APF a ve formátu PDS-E.
thlqual.SCSQCICS	Obsahuje další zaváděcí moduly, které musí být zahrnuty do zřetězení CICS DFHRPL. Tato knihovna musí být autorizovaná APF a ve formátu PDS-E.
thlqual.SCSQCLST	Obsahuje CLISTs používané vzorovými programy.
thlqual.SCSQCOBC	Obsahuje zakladače COBOL, včetně zakladačů požadovaných pro ukázkové programy.
thlqual.SCSQCOBS	Obsahuje zdroj ukázkových programů COBOL.
thlqual.SCSQCPPS	Obsahuje zdroj ukázkových programů C + +.
thlqual.SCSQC37S	Obsahuje zdrojový kód pro ukázkové programy C.

Tabulka 53. Knihovny produktu IBM MQ , které existují po instalaci (pokračování)	
Název	**Popis**
thlqual.SCSQC370	Obsahuje záhlaví C, včetně záhlaví požadovaných pro ukázkové programy.
thlqual.SCSQDEFS	Obsahuje definice strany pro C++ a Db2 DBRM pro sdílené řazení do fronty.
thlqual.SCSQEXEC	Obsahuje spustitelné soubory REXX, které mají být zahrnuty do zřetězení SYSEXEC nebo SYSPROC, pokud používáte operační panely a ovládací panely produktu IBM MQ .
thlqual.SCSQHPPS	Obsahuje hlavičkové soubory pro C + +.
thlqual.SCSQINST	Obsahuje JCL pro instalační úlohy.
thlqual.SCSQLINK	Knihovna předčasného kódu. Obsahuje zaváděcí moduly, které jsou načteny při zavedení inicializačního programu systému (IPL). Knihovna musí být autorizovaná APF.
thlqual.SCSQLOAD	Zaveďte knihovnu. Obsahuje zaváděcí moduly pro kód non-APF, uživatelské procedury, obslužné programy, ukázky, programy pro verifikaci instalace a stuby adaptéru. Knihovna nemusí být APF-autorizována a nemusí být ve spojovacím seznamu. Tato knihovna musí být ve formátu PDS-E.
thlqual.SCSQMACS	Obsahuje makra Assembler včetně: ukázková makra, produktová makra a makra parametrů systému.
thlqual.SCSQMAPS	Obsahuje sady CICS mapset používané ukázkovými programy.
thlqual.SCSQMSGC	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, pokud používáte funkci jazyka Zjednodušená čínština pro operace produktu IBM MQ a řídicí panely.
thlqual.SCSQMSGE	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, používáte-li U.S. Anglická (smíšená) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGF	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, pokud používáte funkci francouzského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGK	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, pokud používáte funkci japonského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQMSGU	Obsahuje zprávy ISPF, které mají být zahrnuty do zřetězení ISPMLIB, používáte-li U.S. Anglická (velká) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQMVR1	Obsahuje zaváděcí moduly pro distribuované řazení do fronty. Tato knihovna musí být autorizovaná APF a ve formátu PDS-E.
thlqual.SCSQPLIC	Obsahuje soubory začlenění PL/I.
thlqual.SCSQPLIS	Obsahuje zdroj ukázkových programů PL/I.
thlqual.SCSQPNLA	Obsahuje panely IPCS, pro formátovač výpisů paměti, které mají být zahrnuty do zřetězení ISPPLIB. Obsahuje také panely s ukázkovými programy produktu IBM MQ .

Tabulka 53. Knihovny produktu IBM MQ , které existují po instalaci (pokračování)	
Název	**Popis**
thlqual.SCSQPNLC	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, pokud používáte funkci jazyka Zjednodušená čínština pro operace produktu IBM MQ a ovládací panely.
thlqual.SCSQPNLE	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, používáte-li U.S. Anglická (smíšená) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQPNLF	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení souboru ISPPLIB, pokud používáte funkci francouzského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQPNLK	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, pokud používáte funkci japonského jazyka pro operace produktu IBM MQ a ovládací panely.
thlqual.SCSQPNLU	Obsahuje panely ISPF, které mají být zahrnuty do zřetězení ISPPLIB, používáte-li U.S. Anglická (velká) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQPROC	Obsahuje ukázkové datové sady JCL a výchozí inicializační datové sady systému.
thlqual.SCSQSNLC	Obsahuje zaváděcí moduly pro zjednodušenou čínskou verzi modulů IBM MQ , které jsou vyžadovány pro funkci speciálního účelu (například pro počáteční kód).
thlqual.SCSQSNLE	Obsahuje zaváděcí moduly pro U.S. Anglická (směs malých a velkých písmen) modulů IBM MQ , které jsou vyžadovány pro speciální účel (například včasný kód).
thlqual.SCSQSNLF	Obsahuje zaváděcí moduly pro francouzské verze modulů IBM MQ , které jsou vyžadovány pro speciální účelovou funkci (například na začátku kódu).
thlqual.SCSQSNLK	Obsahuje zaváděcí moduly pro japonské verze modulů IBM MQ , které jsou vyžadovány pro speciální účelovou funkci (například na začátku kódu).
thlqual.SCSQSNLU	Obsahuje zaváděcí moduly pro U.S. Anglická (velká) verze modulů IBM MQ , které jsou vyžadovány pro funkci speciálního účelu (například včasný kód).
thlqual.SCSQTBLC	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, pokud používáte funkci jazyka Zjednodušená čínština pro operace produktu IBM MQ a řídicí panely.
thlqual.SCSQTBLE	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, používáte-li U.S. Anglická (smíšená) jazyková funkce pro operace IBM MQ a ovládací panely.
thlqual.SCSQTBLF	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, pokud používáte funkci francouzského jazyka pro operace IBM MQ a ovládací panely.
thlqual.SCSQTBLK	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, pokud používáte funkci japonského jazyka pro operace IBM MQ a ovládací panely.

Tabulka 53. Knihovny produktu IBM MQ , které existují po instalaci (pokračování)	
Název	**Popis**
thlqual.SCSQTBLU	Obsahuje tabulky ISPF, které mají být zahrnuty do zřetězení ISPTLIB, používáte-li U.S. Anglická (velká) jazyková funkce pro operace IBM MQ a ovládací panely.

Poznámka: Neupravujte ani neupravujte žádnou z těchto knihoven. Chcete-li provést změny, zkopírujte knihovny a proveďte změny na jejich kopii.

Související pojmy

IBM MQ for z/OS koncepce

“Použití IBM MQ s IMS” na stránce 901
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 909
Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge .

“Použití uživatelských procedur OTMA v adresáři IMS” na stránce 912
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 871
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 na jazykové prostředí nebo z/OS Callable Services” na stránce 909
Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

z/OS nastaveníIBM MQ for z/OS

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ for z/OS .

Nejlepším způsobem, jak nakonfigurovat správce front, je provést následující kroky v uvedeném pořadí:

1. Nakonfigurujte základní správce front.
2. Konfigurujte iniciátor kanálu, který provádí komunikaci správce front s komunikací správce front a komunikaci vzdálených klientských aplikací.
3. Chcete-li šifrovat nebo chránit zprávy, nakonfigurujte prostor 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 administrativní nebo systém zpráv REST APInebo konzolu MQ Console ke správě produktu IBM MQ z webového prohlížeče, nakonfigurujte webový server mqweb.

Toto téma vás provede různými fázemi nastavení produktu IBM MQ poté, co jste jej úspěšně nainstalovali. Proces instalace je popsán v adresáři programu. Program Directory for IBM MQ for z/OS lze stáhnout z adresáře IBM Centrum publikací (viz IBM MQ for z/OS Program Directory PDF files).

Ukázky jsou dodávány s produktem IBM MQ , aby vám pomohly s přizpůsobením. Členové ukázkových datových sad mají názvy začínající na čtyři znaky CSQ4 a jsou v knihovně thlqual.SCSQPROC.

Než provedete úlohy přizpůsobení popsané v tomto tématu, je zde řada voleb konfigurace, které musíte zvážit, protože ovlivňují výkon a požadavky na prostředky produktu IBM MQ for z/OS. Musíte se například rozhodnout, které knihovny globalizace chcete použít.

Chcete-li automatizovat některé kroky přizpůsobení, prohlédněte si téma “Použití produktu IBM z/OSMF k automatizaci IBM MQ” na stránce 916.

Volby konfigurace

Další informace o těchto volbách viz Plánování na z/OS.

Popis každé úlohy v této sekci označuje, zda:

- Úloha je součástí procesu nastavení produktu IBM MQ. To znamená, že provedete úlohu jednou, když upravíte IBM MQ na systému z/OS . (V paralelním prostředí sysplex musíte provést úlohu pro každý systém z/OS v prostředí sysplex a ujistěte se, že každý systém z/OS je nastaven stejně.)
- Úloha je součástí přidání správce front. To znamená, že provedete úlohu jednou pro každého správce front, když přidáte tohoto správce front.

Žádná z úloh nevyžaduje, abyste provedli IPL systému z/OS , pokud používáte příkazy ke změně různých systémových parametrů z/OS , a proveďte “Aktualizujte SYS1.PARMLIB členové” na stránce 814 jak je doporučeno.

Chcete-li zjednodušit operace a usnadnit určování problémů, ujistěte se, že všechny systémy z/OS v prostředí sysplex jsou nastaveny stejně, takže správci front mohou být rychle vytvořen na libovolném systému v nouzi.

Kvůli usnadnění údržby zvažte definování aliasů tak, aby odkazovaly na knihovny produktu IBM MQ ; další informace naleznete v tématu Použití aliasu pro odkaz na knihovnu IBM MQ.

Související pojmy

IBM MQ for z/OS koncepce

“Použití IBM MQ s IMS” na stránce 901
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 909
Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge .

“Použití uživatelských procedur OTMA v adresáři IMS” na stránce 912
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 871
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 na jazykové prostředí nebo z/OS Callable Services” na stránce 909
Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

Související informace

Programový adresář pro IBM MQ for z/OS

z/OS Konfigurace systému z/OS pro produkt IBM MQ

Tato témata popisují krok za krokem pokyny pro přizpůsobení vašeho systému IBM MQ for z/OS .

z/OS *Identifikace systémových parametrů produktu z/OS .*

Některé z úloh zahrnují aktualizaci systémových parametrů produktu z/OS . Musíte vědět, které z nich byly zadány při provádění IPL systému.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*

- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

SYS1.PARMLIB(IEASYSpp) obsahuje seznam parametrů, které odkazují na jiné členy SYS1.PARMLIB (kde pp představuje seznam parametrů systému z/OS , který byl použit k provedení IPL systému).

Položky, které potřebujete najít, jsou:

Pro "Autorizace APF pro zaváděcí knihovny produktu IBM MQ" na stránce 802:
PROG=xx nebo APF=aa, aby ukazovala na seznam autorizovaných knihoven APF (Authorized Program Facility) (člen PROGxx nebo IEFAPFaa)

Pro "Aktualizovat seznam odkazů z/OS a LPA" na stránce 803:
LNK=kk ukazuje na seznam propojení (člen LNKLSTkk) LPA=mm ukazuje na seznam LPA (člen LPALSTmm)

Pro "Aktualizace tabulky vlastností programu z/OS" na stránce 807:
SCH=xx ukazuje na tabulku vlastností programu (PPT) (člen SCHEDxx)

Pro "Definujte subsystém IBM MQ na z/OS" na stránce 807:
SSN=ss ukazuje na definovaný seznam subsystémů (člen IEFSSNss)

z/OS *Autorizace APF pro zaváděcí knihovny produktu IBM MQ*

APF-autorizovat různé knihovny. Některé zaváděcí moduly již mohou být autorizovány.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že jsou nastavení pro IBM MQ identická na každém systému z/OS v prostředí sysplex.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*
- *Použití knihovny Look stranou (LLA):*
  - *Některé využití IBM MQ mohou způsobit načtení modulů z knihoven s vysokým vstupem/výstupem (I/O). Tento I/O lze snížit pomocí poskytované služby LLA operačního systému.*
  - *Tento vysoký vstup/výstup se může vyskytnout během:*
    - *Aplikace s vysokou četností MQCONN/MQDISC, například v uložené proceduře WLM.*
    - *Probíhá načítání kanálů kanálu. Máte-li kanály, které spouštějí a zastavují často, a používají uživatelské procedury kanálu.*
  - *Člen CSVLLAxx v SYS1.PARMLIB určuje nastavení LLA. Začlenění názvu knihovny do příkazu LIBRARIES znamená, že kopie programu bude vždy převzata z VLF (Virtual Lookaside Facility), a proto nebude obvykle vyžadovat I/O, když je intenzivně využíván.*

    Inclusion in the FREEZE statement means that there is no I/O to get the relevant DD příkaz concatenation directories (this can often be more I/O than the program load itself).

    Použijte příkaz operačního systému " F LLA, REFRESH " after any changes to any of these libraries.

Zaváděcí knihovny IBM MQ thlqual.SCSQAUTH a thlqual.SCSQLINK musí mít oprávnění APF-. Musíte také APF autorizovat knihovny pro funkci národního jazyka (thlqual.SCSQANLx a thlqual.SCSQSNLx) a pro funkci distribuovaných front (thlqual.SCSQMVR1). Pokud používáte Advanced Message Security , musíte také autorizovat APF pro knihovnu thlqual.SDRQAUTH.

Nicméně všechny zaváděcí moduly v LPA jsou automaticky autorizovány APF. Jsou-li tedy SYS1.PARMLIB člen IEASYSpp obsahuje následující příkaz:

```
LNKAUTH=LNKLST
```

LNKAUTH=LNKLST je předvolba, pokud není uvedeno LNKAUTH.

V závislosti na tom, co vyberete pro vložení do LPA nebo seznamu odkazů (viz “Aktualizovat seznam odkazů z/OS a LPA” na stránce 803), možná nebudete muset umístit knihovny do seznamu odkazů APF

Poznámka: Musíte APF autorizovat všechny knihovny, které zahrnete do STEPLIB produktu IBM MQ . Pokud vložíte do STEPLIB knihovnu, která není autorizována APF, ztratí zřetězení knihovny autorizaci APF.

Seznamy APF jsou v SYS1.PARMLIB member PROGxx nebo IEAAPFaa. Seznamy obsahují názvy autorizovaných knihoven z/OS APF. Pořadí položek v seznamech není významné. Informace o seznamech APF najdete v příručce *z/OS MVS Initialization and Tuning Reference* .

Další informace o ladění systému najdete v tématu SupportPac MP16 .

Pokud použijete členy PROGxx s dynamickým formátem, musíte vydat pouze příkaz z/OS SETPROG `APF,ADD,DSNAME=hlq.SCSQ XXXX,VOLUME= YYYYYY` , aby se změny projevily: Kde *XXXX* se liší podle názvu knihovny a kde *YYYYY* je hlasitost. Jinak, pokud používáte statický formát nebo IEAPFaa členy, musíte provést IPL na systému.

Všimněte si, že musíte použít skutečný název knihovny v seznamu APF. Pokusíte-li se použít alias datové sady knihovny, autorizace selže.

Související pojmy

“Aktualizovat seznam odkazů z/OS a LPA” na stránce 803
Aktualizujte knihovny LPA pomocí nové verze knihoven s časným kódem. Ostatní kódy mohou být uvedeny v seznamu odkazů nebo v oblasti LPA.

“Příprava na přizpůsobení správců front v systému z/OS” na stránce 796
Toto téma vám pomůže při přizpůsobování správců front s podrobnými informacemi o instalovatelných funkcích, národním jazykovým funkcím a informacím o testování a nastavení zabezpečení.

z/OS *Aktualizovat seznam odkazů z/OS a LPA*

Aktualizujte knihovny LPA pomocí nové verze knihoven s časným kódem. Ostatní kódy mohou být uvedeny v seznamu odkazů nebo v oblasti LPA.

- Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.
- Používáte-li skupiny sdílení front, měli byste před migrací libovolného správce front do produktu IBM MQ 9.1.0aktualizovat dřívější kód v každém správci front na úrovni IBM MQ 9.1.0 .

  Nainstalujte nejnovější kód v každé logické oblasti LPAR a poté před migrací aktualizujte správce front jednu po druhé v určitém okamžiku. Nemusíte migrovat všechny správce front zároveň.
- Možná budete muset provést tuto úlohu při migraci z předchozí verze. Další informace najdete v tématu Adresář programu. Program Directory for IBM MQ for z/OS lze stáhnout z adresáře IBM Centrum publikací (viz IBM MQ for z/OS Program Directory PDF files).

Poznámka: Datová sada pro LPA je specifická pro verzi. Pokud používáte existující LPA v systému, obraťte se na administrátora systému, aby rozhodl, který server LPA se má použít.

Předčasný kód

Některé zaváděcí moduly produktu IBM MQ je třeba přidat do produktu MVS for IBM MQ , aby se mohli chovat jako subsystém. Tyto moduly jsou známy jako úvodní kód a lze je spouštět i v případě, že správce front není aktivní. Je-li například na konzole zadán příkaz operátora s předponou příkazu IBM MQ , tento Early kód získá kontrolu a zkontroluje, zda potřebuje spustit správce front, nebo předat požadavek spuštěnému správci front. Tento kód je načten do oblasti LPA (Link Pack Area). Existuje jedna sada Early modulů, které se používají pro všechny správce front, a ty je třeba mít na nejvyšší úrovni IBM MQ. Early code from a higher version of IBM MQ will work with a queue manager with a lower version of IBM MQ, but not the opposite.

První kód se skládá z následujících modulů zatížení:

- CSQ3INI a CSQ3EPX v knihovně thqual.SCSQLINK
- CSQ3ECMX v knihovně thqual.SCSQSNL *x*, kde *x* je váš jazykový dopis:
  - thlqual.SCSQSNLE, v případě smíšených velkých a malých písmen v angličtině

- thlqual.SCSQSNLU, pro americká angličtina, velká písmena
- thlqual.SCSQSNLK, pro japonštinu
- thlqual.SCSQSNLF, pro francouzštinu
- thlqual.SCSQSNLC, pro čínštinu

Produkt IBM MQ zahrnuje úpravu uživatele, která přesouvá obsah knihovny thqual.SCSQSNL *i* do souboru thqual.SCSQLINK a informuje SMP/E. Tato změna uživatele se nazývá CSQ8UERL a je popsána v adresáři *Program Directory for IBM MQ for z/OS* buď pro Long Term Support , nebo pro Continuous Delivery. Program Directory for IBM MQ for z/OS lze stáhnout z adresáře IBM Centrum publikací (viz IBM MQ for z/OS Program Directory PDF files).

When you have updated the early code in the LPA libraries, it is available from the next z/OS IPL (with the CLPA option) to all queue manager subsystems added during IPL from definitions in IEFSSNss members in SYS1.PARMLIB.

Můžete ji zpřístupnit okamžitě bez provedení IPL pro každý nový subsystém správce front přidaný později (jak je popsáno v tématu “Definujte subsystém IBM MQ na z/OS” na stránce 807). přidáním do LPA takto:

- Pokud jste nepoužili CSQ8UERL, zadejte tyto příkazy z/OS :

```
SETPROG LPA,ADD,MODNAME=(CSQ3INI,CSQ3EPX),DSNAME=thqual.SCSQLINK
SETPROG LPA,ADD,MODNAME=(CSQ3ECMX),DSNAME=thqual.SCSQSNL x
```

- Pokud jste použili CSQ8UERL, můžete do LPA načíst počáteční kód pomocí následujícího příkazu z/OS :

```
SETPROG LPA,ADD,MASK=*,DSNAME=thqual.SCSQLINK
```

- Pokud používáte Advanced Message Security , musíte také vydat následující příkaz z/OS , aby zahrnoval další modul v LPA:

```
SETPROG LPA,ADD,MODNAME=(CSQ0DRTM),DSNAME=thqual.SCSQLINK
```

Pokud jste použili údržbu nebo chcete restartovat správce front s novější verzí nebo verzí produktu IBM MQ, je možné počáteční kód zpřístupnit existujícím správcům front pomocí následujících kroků. Správci front, kteří tyto kroky neprovádějí, jsou nadále používány verzí předčasného kódu, který již používají. Není nutné provádět tyto kroky pro všechny správce front v logické oblasti (LPAR), pokud se specificky nesnažíte použít údržbu na všechny správce nebo je aktualizovat vše na novější verzi nebo vydání produktu IBM MQ.

1. Přidejte jej do LPA pomocí příkazů z/OS SETPROG, jak je popsáno výše v tomto tématu.
2. Zastavte správce front pomocí příkazu IBM MQ STOP QMGR.
3. Ujistěte se, že qmgr.REFRESH.QMGR je nastaven. Viz příkazy MQSC, profily a jejich úrovně přístupu.
4. Aktualizujte počáteční kód pro správce front pomocí příkazu IBM MQ REFRESH QMGR TYPE (EARLY).
5. Restartujte správce front pomocí příkazu IBM MQ START QMGR.

Příkazy IBM MQ STOP QMGR, REFRESH QMGR a START QMGR jsou popsány v příkazech MQSC.

Jiný kód

Všechny zaváděcí moduly dodané IBM MQ v následujících knihovnách jsou reentrantní a lze je umístit do LPA:

- SCSQAUTH
- SCSQANL *x*, kde *x* je váš jazykový dopis
- SCSQMVR1

Důležité: Pokud však umístíte knihovny do LPA, kdykoli použijete údržbu, budete muset ručně okopírovat všechny změněné moduly do LPA. Proto je vhodnější umístit zaváděcí knihovny produktu IBM MQ do seznamu odkazů, které lze aktualizovat po údržbě zadáním příkazu z/OS REFRESH LLA.

To je zvláště doporučeno pro SCSQAUTH, takže je nemusíte zahrnout do několika STEPLIBs. Pouze jedna jazyková knihovna, SCSQANL *x* by měla být umístěna v seznamu LPA nebo seznamu odkazů. Knihovny seznamu odkazů jsou uvedeny v členu LNKLSTkk členu SYS1.PARMLIB.

Distribuované zařízení pro práci s frontami a produkt CICS bridge (nikoli však samotný správce front) potřebují přístup ke knihovně běhových prostředí SCEERUN běhového prostředí jazyka LE (Language Environment). Pokud použijete kterýkoli z těchto zařízení, musíte zahrnout SCEERUN do seznamu odkazů.

Některé moduly jsou načteny při spuštění správce front do produktu ECSA. V prostředích ECSA s omezeným prostředím je možné místo toho umístit tyto moduly do LPA. Další informace viz "Umístění globálních modulů IBM MQ do LPA" na stránce 805.

Důležité: Chcete-li použít tuto poskytovanou službu v produktu IBM MQ 9.1 , je třeba použít opravu APAR PH52358.

Související pojmy

"Aktualizace tabulky vlastností programu z/OS" na stránce 807
Pro správce front produktu IBM MQ jsou zapotřebí některé další položky PPT.

z/OS *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.

Důležité: Chcete-li použít toto zařízení v produktu IBM MQ 9.1 , musíte použít opravu APAR PH52358.

K dispozici je 19 globálních modulů, které v produktu IBM MQ 9.1spotřebovávají přibližně 1.2 MB ECSA na spuštěného správce front. V prostředích, která spouštějí více správců front na oblast LPAR a vyžadují snížení spotřeby ECSA kvůli ECSA nebo vysokým soukromým omezením, je možné umístit globální moduly do LPA.

Poznámka: Ačkoli je CSQ7GPLM globální modul, neměl by být přidán do LPA.

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.

Společná funkce sledování úložiště systému z/OS (viz Použití společné funkce sledování úložiště) sleduje úložiště pod adresním prostorem MSTR jednotlivých správců front a lze ji použít ke zjištění, kolik prostoru využívají globální moduly.

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

Notes:

- 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 produktu IBM MQ” na stránce 802.
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 803
Aktualizujte knihovny LPA pomocí nové verze knihoven s časným kódem. Ostatní kódy mohou být uvedeny v seznamu odkazů nebo v oblasti LPA.

z/OS *Aktualizace tabulky vlastností programu z/OS*

Pro správce front produktu IBM MQ jsou zapotřebí některé další položky PPT.

- *Tuto úlohu musíte provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že jsou nastavení pro IBM MQ identická na každém systému z/OS v prostředí sysplex.*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*
- *Chcete-li vyžadovat produkt Advanced Message Security, musíte provést část CSQ0DSRV této úlohy.*

Ukázka obsahující všechny požadované položky PPT je poskytnuta v souboru thlqual.SCSQPROC(CSQ4SCHD). Ujistěte se, že jsou požadované záznamy přidány do PPT, které můžete najít v SYS1.PARMLIB(SCHEDxx).

V produktu z/OS 1.12 a v novějších verzích je CSQYASCP již definován pro operační systém s atributy detailními a již nemusí být zahrnuti do členu SCHEDxx oblasti PARMLIB.

Správce front produktu IBM MQ řídí výměnu sebe sama. Pokud však máte silně zatížené IBM MQ sítě a doba odezvy je kritická, může být výhodné nastavit iniciátor kanálu IBM MQ nespojovatelným přidáním položky CSQXJST PPT, a to s rizikem ovlivnění výkonu zbytku vašeho systému z/OS .

Požadujete-li Advanced Message Security, přidejte položku PPT CSQ0DSRV .

Vydejte příkaz z/OS **SET SCH=xx**, kde *xx* je přípona členu SCHEDxx knihovny PARMLIB, aby se tyto změny projevily.

Související pojmy

“Definujte subsystém IBM MQ na z/OS” na stránce 807
Aktualizujte tabulku názvů subsystémů a rozhodněte se podle konvence pro řetězce předpony příkazu.

z/OS Konfigurace správce front a inicializátoru kanálu

Tato témata můžete použít jako krok za krokem ke konfiguraci správce front a inicializátoru kanálu.

z/OS *Definujte subsystém IBM MQ na z/OS*

Aktualizujte tabulku názvů subsystémů a rozhodněte se podle konvence pro řetězce předpony příkazu.

Opakujte tuto úlohu pro každého správce front produktu IBM MQ . Při migraci z předchozí verze není třeba tuto úlohu provést.

Související pojmy

“Vytvoření procedur pro správce front produktu IBM MQ” na stránce 811
Každý subsystém IBM MQ potřebuje katalogovou proceduru ke spuštění správce front. Můžete vytvořit vlastní nebo použít knihovnu procedur dodané s produktem IBM.

z/OS *Aktualizace tabulky názvů subsystémů*

Při definování subsystému IBM MQ je třeba přidat položku do tabulky názvů subsystémů.

Tabulka názvů subsystémů produktu z/OS, která je původně brána z SYS1.PARMLIB Člen IEFSSNss, obsahuje definice formálně definovaných subsystémů z/OS . Chcete-li definovat každý subsystém IBM MQ , musíte do této tabulky přidat položku, a to buď změnou člena IEFSSNss SYS1.PARMLIB, nebo pokud možno, pomocí příkazu z/OS SETSSI.

Inicializace subsystému IBM MQ podporuje paralelní zpracování, takže lze do tabulky IEFSSNss v tabulce IEFSSNss, která je k dispozici na serveru z/OS V1.12 , a později, přidat příkazy definice subsystému IBM MQ , a to jak nad a pod klíčovým slovem BEGINPARALLEL.

Použijete-li příkaz SETSSI, změna se projeví okamžitě a není třeba provádět IPL systému. Ujistěte se, že aktualizujete SYS1.PARMLIB stejně tak, jak je popsáno v tématu “Aktualizujte SYS1.PARMLIB členové” na stránce 814 , takže změny zůstávají v platnosti po následných IPL.

Příkaz SETSSI pro dynamické definování subsystému IBM MQ je následující:

```
SETSSI ADD,S=ssid,I=CSQ3INI,P='CSQ3EPX,cpf,scope'
```

Odpovídající informace v IEFSSNss lze zadat jedním ze dvou způsobů:

- Formát parametru klíčového slova v definici subsystému IBM MQ v IEFSSNss. Toto je doporučená metoda.

  ```
  SUBSYS SUBNAME(ssid) INITRTN(CSQ3INI) INITPARM('CSQ3EPX,cpf,scope')
  ```

- Poziční parametr z definice subsystému IBM MQ .

  ```
  ssid,CSQ3INI,'CSQ3EPX,cpf,scope'
  ```

Nesměšujte tyto dva formuláře v jednom členu IEFSSNss. Pokud jsou vyžadovány různé formuláře, použijte oddělený člen IEFSSNss pro každý typ, přidáním operandu SSN nového člena do IEASYSpp SYS1.PARMLIB . Chcete-li určit více než jednu společnost SSN, použijte společnost SSN = (aa, bb, ...) v IEASYSpp.

V příkladech:

ssid
: Identifikátor subsystému. Může mít délku až čtyři znaky. Všechny znaky musí být alfanumerické (velká písmena A až Z, 0 až 9), musí začínat abecedním znakem. Správce front bude mít stejný název jako subsystém, a proto můžete použít pouze znaky, které jsou povoleny pro názvy subsystémů z/OS i názvy objektů produktu IBM MQ .

cpf
: Řetězec předpony příkazu (informace o CPF naleznete v příručce “Definování řetězců s předponou příkazu (CPF)” na stránce 809).

scope
: Rozsah systému, použitý, pokud pracujete v prostředí sysplex z/OS (informace o rozsahu systému viz “Kódy CPF v prostředí sysplex” na stránce 810).

Příkaz Obrázek 99 na stránce 808 zobrazuje několik příkladů příkazů IEFSSNss.

```
CSQ1,CSQ3INI,'CSQ3EPX,+mqs1cpf,S'
CSQ2,CSQ3INI,'CSQ3EPX,+mqs2cpf,S'
CSQ3,CSQ3INI,'CSQ3EPX,++,S'
```

Obrázek 99. Ukázka příkazů IEFSSNss pro definování subsystémů

Poznámka: Pokud jste v subsystému vytvořili objekty, nemůžete změnit název subsystému nebo použít sady stránek z jednoho subsystému v jiném subsystému. Chcete-li provést některou z těchto úloh, je nutné uvolnit všechny objekty a zprávy z jednoho subsystému a znovu je načíst do jiného subsystému.

Tabulka 54 na stránce 809 udává počet příkladů, které zobrazují přidružení názvů subsystémů a řetězců s předponou příkazu, jak je definováno příkazy v Obrázek 99 na stránce 808.

Tabulka 54. Název subsystému pro přidružení CPF

Název podsystému IBM MQ	**CPF**
CSQ1	+mqs1cpf
CSQ2	+mqs2cpf
CSQ3	++

Poznámka: Funkce ACTIVATE a DEACTIVATE příkazu z/OS SETSSI nejsou podporovány produktem IBM MQ.

Chcete-li zkontrolovat stav těchto změn, zadejte následující příkaz v SDSF: `/D SSI,L`. Zobrazí se nové subsystémy vytvořené ve stavu AKTIVNÍ.

z/OS *Definování řetězců s předponou příkazu (CPF)*

Každá instance subsystému IBM MQ může mít řetězec předpony příkazu k identifikaci tohoto subsystému.

Převzetí celosystémové konvence pro vaše CPF pro všechny subsystémy, aby nedocházelo ke konfliktům. Dodržujípokyny k následujícím pokynům:

- Definujte CPF jako řetězec o délce až osmi znaků.
- Nepoužívejte CPF, který je již používán jiným podsystémem, a vyvarujte se použití znaku backspace JES definovaného ve vašem systému jako prvního znaku vašeho řetězce.
- Definujte CPF pomocí znaků ze sady platných znaků vypsaných v Tabulka 56 na stránce 810.
- Nepoužívejte CPF, který je zkratka pro již definovaný proces, nebo který může být zaměňován s syntaxí příkazu. Například, CPF jako 'D' conflicts with z/OS commands such as' DISPLAY. Chcete-li se tomuto problému vyhnout, použijte jeden ze speciálních znaků (viz Tabulka 56 na stránce 810). 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 809.

Tabulka 55. Příklad dílčí sady CPF a pravidel supersady

Název podsystému	**Definované CPF**	**Příkazy směrované do**
MQA	!A	MQA
MQB	!B	MQB
MQC1	!C1	MQC1
MQC2	!C2	MQC2
MQB1	!B1	MQB

Příkazy určené pro subsystém MQB1 (použití CPF!)B1) jsou 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
```

(který se v tomto případě nemůže vypořádat s).

Chcete-li zjistit, které předpony existují, zadejte příkaz z/OS DISPLAY OPDATA.

Pokud pracujete v prostředí sysplex, produkt z/OS diagnostikuje všechny konflikty tohoto typu v době registrace CPF (viz “Kódy CPF v prostředí sysplex” na stránce 810 , kde získáte informace o registraci CPF).

Tabulka 56 na stránce 810 ukazuje 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 a až z
Číselné	0 až 9
Národní (viz poznámka)	@ $# (znaky, které mohou být reprezentovány jako hexadecimální hodnoty)
Speciální	. □ ( ) * & + - = ¢ < | ! ; % _ ? : >

Poznámka:

Systém rozpoznává následující hexadecimální reprezentace národních znaků: @ jako X'7C', $jako X'5B' a # jako X'7B'. V jiných zemích, než je U.S. U.S. Národní znaky znázorněné na klávesnicích terminálu mohou generovat jinou hexadecimální reprezentaci a způsobit chybu. Například v některých zemích může znak $generovat symbol '4A'.

Středník (;) je platný jako CPF, ale ve většině systémů tento znak je oddělovač příkazů.

z/OS *Kódy CPF v prostředí sysplex*

Toto téma vám pomůže porozumět způsobu použití rozhraní CPF v rámci oboru prostředí sysplex.

Pokud se používá v prostředí sysplex, IBM MQ registruje vaše CPF, aby vám umožnil zadat příkaz z libovolné konzoly v prostředí sysplex a směrovat tento příkaz na vhodný systém pro provedení. Odezvy příkazu se vrátí na původní konzolu.

Definování rozsahu pro operaci prostředí sysplex

Rozsah se používá k určení typu registrace CPF prováděné subsystémem IBM MQ , když provozujete produkt IBM MQ v prostředí sysplex.

Možné hodnoty rozsahu jsou následující:

M

Rozsah systému.

CPF je registrován s z/OS v době IPL systému produktem IBM MQ a zůstává registrován pro celou dobu, kdy je systém z/OS aktivní.

Příkazy IBM MQ musí být zadávána na konzole připojené k obrazu z/OS , kde je spuštěn cílový subsystém, nebo musíte použít příkazy ROUTE pro přesměrování příkazu na tento obraz.

Tuto volbu použijte, pokud není spuštěna v prostředí sysplex.

S

Byl spuštěn rozsah prostředí sysplex.

CPF je registrován u z/OS při spuštění podsystému IBM MQ a zůstává aktivní, dokud se subsystém IBM MQ neukončí.

Chcete-li směrovat původní příkaz START QMGR na cílový systém, musíte použít příkazy ROUTE, ale všechny další příkazy IBM MQ lze zadat na libovolné konzoli připojené k prostředí sysplex a jsou směrovány do cílového systému automaticky.

Po ukončení IBM MQ musíte použít příkazy ROUTE pro směrování následných příkazů START do cílového subsystému IBM MQ .

X

Rozsah IPL prostředí sysplex.

CPF je registrován s z/OS v době IPL systému produktem IBM MQ a zůstává registrován pro celou dobu, kdy je systém z/OS aktivní.

Příkazy IBM MQ lze zadat na libovolné konzoli připojené k prostředí sysplex a jsou směrovány na obraz, který automaticky provádí cílový systém.

Subsystém IBM MQ s rozsahem CPF s rozsahem S může být definován na jednom nebo více obrazů z/OS v prostředí sysplex, takže tyto obrazy mohou sdílet jednu tabulku názvů subsystémů. Musíte však zajistit, aby počáteční příkaz START byl zadán (nebo přesměrován na) obraz z/OS , na kterém má být spuštěn subsystém IBM MQ . Použijete-li tuto volbu, můžete zastavit subsystém IBM MQ a restartovat jej na jiném obrazu produktu z/OS v rámci prostředí sysplex, aniž byste museli měnit tabulku názvů subsystémů nebo provádět IPL systému z/OS .

Subsystém IBM MQ s rozsahem CPF s rozsahem X může být definován pouze na jednom obrazu z/OS v rámci prostředí sysplex. Použijete-li tuto volbu, musíte definovat jedinečnou tabulku názvů subsystémů pro každý obraz produktu z/OS , který vyžaduje IBM MQ subsystémů s hodnotami CPF rozsahu X.

Chcete-li správce automatického restartu produktu z/OS (ARM) použít k automatickému restartování správců front v různých obrazech produktu z/OS , musí být každý správce front definován v každém obrazu produktu z/OS , na kterém může být správce front restartován. Každý správce front musí být definován se systémem sysple-wide, jedinečným 4znakový název subsystému s rozsahem CPF.

z/OS *Vytvoření procedur pro správce front produktu IBM MQ*

Každý subsystém IBM MQ potřebuje katalogovou proceduru ke spuštění správce front. Můžete vytvořit vlastní nebo použít knihovnu procedur dodané s produktem IBM.

- Opakujte tuto úlohu pro každého správce front produktu IBM MQ .
- Při migraci z předchozí verze může být nutné upravit katalogizovanou proceduru.

U každého subsystému IBM MQ definovaného v tabulce názvů subsystémů vytvořte katalogizovanou proceduru v knihovně procedur pro spuštění správce front. Knihovna procedur dodaných IBMse nazývá SYS1.PROCLIB, ale vaše instalace může používat vlastní konvenci pojmenování.

Název procedury spuštěné úlohy správce front je vytvořen zřetězením názvu subsystému se znaky MSTR. Subsystém CSQ1 má například název procedury CSQ1MSTR. Potřebujete jeden postup pro každý subsystém, který definujete.

Je třeba zahrnout knihovnu obsahující zprávy ve zvoleném jazyce:

- thlqual.SCSQSNLE, v případě smíšených velkých a malých písmen v angličtině
- thlqual.SCSQSNLU, pro americká angličtina, 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 se mohou snáze používat, je-li subsystém s názvem CSQ1 původně vytvořen pro verifikaci instalace a testovací účely.

V souboru thlqual.SCSQPROCjsou k dispozici dva ukázkové procedury spuštění ukázky. Člen CSQ4MSTR používá jednu sadu stránek pro každou třídu zprávy, člen CSQ4MSRR používá více sad stránek pro hlavní třídy zprávy. Zkopírujte jednu z těchto procedur do členu xxxxMSTR (kde xxxx je název vašeho subsystému IBM MQ) vaší SYS1.PROCLIB nebo, pokud nepoužíváte SYS1.PROCLIB, vaše knihovna

procedur. Zkopírujte vzorovou proceduru na člena v knihovně procedur pro každý definovaný subsystém IBM MQ .

Když jste členy zkopírovali, můžete je přizpůsobit požadavkům jednotlivých subsystémů, a to za použití pokynů v členu. Informace o určení omezení úložiště používaného správcem front najdete v tématu Doporučené velikosti oblastí. Symbolické parametry v souboru JCL můžete také použít k povolení úpravy procedury při jeho spuštění. Máte-li několik subsystémů IBM MQ , můžete zjistit, že je výhodné použít JCL pro společné části postupu, aby se zjednodušila budoucí údržba.

Pokud používáte skupiny sdílení front, zřetězení STEPLIB musí zahrnovat cílovou knihovnu běhového prostředí produktu Db2 SDSNLOAD a musí být autorizováno APF. Tato knihovna je vyžadována pouze v zřetězení STEPLIB, pokud není přístupný prostřednictvím seznamu odkazů nebo LPA.

Pokud používáte Advanced Message Security zřetězení STEPLIB, musí obsahovat *thlqual*.SDRQAUTH a musí mít autorizaci APF.

Poznámka: Můžete vytvořit poznámku názvů sady BSDS (bootstrap data set), protokolů a sad stránek pro použití v souboru JCL a poté definovat tyto sady v pozdějším kroku v procesu.

Související pojmy

"Vytvořit procedury pro inicializátor kanálu" na stránce 812
Pro každý subsystém IBM MQ krejte kopii CSQ4CHIN. V závislosti na tom, jaké další produkty používáte, může být třeba povolit přístup k jiným datovým sadám.

z/OS *Vytvořit procedury pro inicializátor kanálu*

Pro každý subsystém IBM MQ krejte kopii CSQ4CHIN. V závislosti na tom, jaké další produkty používáte, může být třeba povolit přístup k jiným datovým sadám.

- Opakujte tuto úlohu pro každého správce front produktu IBM MQ .
- Při migraci z předchozí verze může být nutné upravit katalogizovanou proceduru.

Je třeba vytvořit proceduru spuštěné úlohy iniciátoru kanálu pro každý subsystém IBM MQ , který bude používat distribuované řazení do fronty.

Postupujte takto:

1. Zkopírujte ukázkovou spuštěnou proceduru úlohy thlqual.SCSQPROC(CSQ4CHIN) do knihovny procedur. Pojmenujte proceduru *xxxx* CHIN, kde *xxxx* je název vašeho subsystému IBM MQ (například CSQ1CHIN by byla procedura spuštění úlohy iniciátoru kanálu pro správce front CSQ1).
2. Vytvořte kopii pro každý subsystém IBM MQ , který budete používat.
3. Přizpůsobte postupy dle vašich požadavků podle pokynů v ukázkové proceduře CSQ4CHIN. Symbolické parametry v souboru JCL můžete také použít k povolení úpravy procedury při jeho spuštění. Tento popis je popsán spolu s volbami spuštění v části Administrace produktu IBM MQ for z/OS.

   Zřetězete distribuovanou knihovnu front thlqual.SCSQMVR1.

   Je požadován přístup ke knihovně běhového prostředí LE SCEERUN; pokud není uveden ve vašem seznamu odkazů (SYS1.PARMLIB(LNKLSTkk)), zřetězte jej v příkazu STEPLIB DD.
4. Autorizujte procedury pro spuštění pod vaším externím správcem zabezpečení.
5. Je třeba zahrnout knihovnu obsahující zprávy ve zvoleném jazyce:
   - thlqual.SCSQSNLE, v případě smíšených velkých a malých písmen v angličtině
   - thlqual.SCSQSNLU, pro americká angličtina, velká písmena
   - thlqual.SCSQSNLK, pro japonštinu
   - thlqual.SCSQSNLF, pro francouzštinu
   - thlqual.SCSQSNLC, pro čínštinu

Inicializátor kanálu je dlouhý spuštěný adresový prostor. Chcete-li zabránit jejímu ukončení po spotřebování omezeného množství CPU, potvrďte, že buď:

- Předvolba pro spuštěné úlohy ve vašem systému z/OS je neomezená CPU; konfigurační příkaz JES2 pro JOBCLASS (STC) s TIME = (1440,00) jej dosáhne, nebo
- Explicitně přidejte parametr TIME=1440, nebo TIME=NOLIMIT, do příkazu EXEC pro CSQXJST.

Knihovnu uživatelské procedury (CSQXLIB) můžete do této procedury přidat později, chcete-li použít uživatelské procedury kanálu. Chcete-li to provést, musíte zastavit a restartovat iniciátor kanálu.

Používáte-li TLS, je vyžadována přístupová práva k systémové knihovně běhového prostředí TLS. Tato knihovna se jmenuje SIEALKE. Knihovna musí mít oprávnění APF.

Pokud používáte protokol TCP/IP, musí být adresní prostor inicializátoru kanálu schopen získat přístup k protokolu TCPIP.DATA datová sada, která obsahuje parametry systému TCP/IP. Způsob, jakým má být datová sada nastavena, závisí na tom, který produkt a rozhraní TCP/IP používáte. Mezi ně patří:

- Proměnná prostředí, RESOLERVER_CONFIG
- /etc/resolv.conf v systému souborů
- // SYSTCPD DD, příkaz
- // SYSTCPDD DD, příkaz
- *jobname/userid*.TCPIP.DATA
- SYS1.TCPPARMS(TCPDATA)
- *zapname*.TCPIP.DATA

Některé z nich mají vliv na kód JCL procedury spouštěné úlohy. Další informace viz z/OS Communications Server: IP Configuration Guide.

Související pojmy

“Definujte subsystém IBM MQ k třídě služeb z/OS WLM.” na stránce 813
Chcete-li v systému z/OS udělit IBM MQ odpovídající prioritu výkonu, musíte přiřadit adresní prostory správce front a inicializátoru kanálu k příslušné třídě služeb správy pracovní zátěže (WLM) produktu z/OS . Pokud to neuděláte explicitně, může se použít nevhodná výchozí nastavení.

z/OS *Definujte subsystém IBM MQ k třídě služeb z/OS WLM.*

Chcete-li v systému z/OS udělit IBM MQ odpovídající prioritu výkonu, musíte přiřadit adresní prostory správce front a inicializátoru kanálu k příslušné třídě služeb správy pracovní zátěže (WLM) produktu z/OS . Pokud to neuděláte explicitně, může se použít nevhodná výchozí nastavení.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*

Pomocí dialogového okna ISPF dodaného s modulem WLM lze provádět následující úlohy:

- Extrahujte definici zásady správce WLM produktu z/OS z dvojice datových sad WLM.
- Aktualizujte tuto definici zásady přidáním názvů procedur spuštěných úloh iniciátoru správce front a inicializátoru kanálu do vybrané třídy služeb.
- Nainstalujte změněnou zásadu do dvojice datových sad WLM.

Poté aktivujte tuto zásadu pomocí příkazu z/OS .

```
V WLM,POLICY=policyname,REFRESH
```

Další informace o nastavení voleb výkonu najdete v tématu Plánování prostředí IBM MQ v systému z/OS .

Související pojmy

“Nastavení prostředí produktu Db2” na stránce 848
Používáte-li skupiny sdílení front, musíte vytvořit požadované objekty produktu Db2 přizpůsobením a spuštěním počtu ukázkových úloh.

z/OS *Provádět ovládací prvky zabezpečení ESM*

Implementujte obslužné prvky zabezpečení pro správce front a inicializátor kanálu.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Pokud používáte produkt RACF jako externího správce zabezpečení, přečtěte si téma Nastavení zabezpečení v produktu z/OS , které popisuje, jak implementovat tyto ovládací prvky zabezpečení.

Pokud používáte inicializátor kanálu, je třeba provést také následující akce:

- Pokud má váš subsystém aktivní zabezpečení připojení, definujte profil zabezpečení připojení ssid.CHIN do svého externího správce zabezpečení (informace o tomto tématu naleznete v tématu Profily zabezpečení připojení pro inicializátor kanálu).
- Pokud používáte TLS (Transport Layer Security) nebo soketové rozhraní, ujistěte se, že ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je konfigurován tak, aby používal produkt UNIX System Services, jak je popsáno v dokumentaci *OS/390 UNIX System Services Planning* .
- Pokud používáte TLS, ujistěte se, že ID uživatele, pod jehož oprávněním je spuštěn inicializátor kanálu, je konfigurován pro přístup k souboru svazku klíčů uvedenému v parametru SSLKEYR příkazu ALTER QMGR.

Před spuštěním správce front nastavte IBM MQ datovou sadu a zabezpečení systému pomocí:

- Autorizací procedury spuštěné úlohy správce front pro spuštění pod vaším externím správcem zabezpečení.
- Autorizování přístupu k datovým sadám správce front.
- V 9.1.4 Je-li to nutné, konfigurace šifrování dat produktu z/OS .

  Informace naleznete v části Důvěrnost dat v produktu IBM MQ for z/OS s šifrováním datové sady. Další informace viz.

Podrobnosti o tom, jak to provést, najdete v tématu Úlohy instalace zabezpečení pro produkt z/OS.

Pokud používáte produkt RACF, za předpokladu, že použijete třídu RACF STARTED, není nutné provádět IPL systému (viz RACF autorizace spuštěných procedur úloh).

Související pojmy

“Aktualizujte SYS1.PARMLIB členové” na stránce 814
Chcete-li se ujistit, že vaše změny zůstanou v platnosti po IPL, musíte aktualizovat některé členy SYS1.PARMLIB

“Implementovat ovládací prvky zabezpečení ESM pro skupinu sdílení front” na stránce 852
Implementujte ovládací prvky zabezpečení pro všechny správce front ve skupině sdílení front, přístup k serveru Db2 a ke strukturám seznamu prostředků Coupling Facility.

z/OS *Aktualizujte SYS1.PARMLIB členové*

Chcete-li se ujistit, že vaše změny zůstanou v platnosti po IPL, musíte aktualizovat některé členy SYS1.PARMLIB

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Pokud používáte skupiny sdílení front, musíte se ujistit, že jsou nastavení pro IBM MQ identická na každém systému z/OS v prostředí sysplex.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Aktualizujte SYS1.PARMLIB :

1. Aktualizujte člen IEFSSNss, jak je popsáno v tématu “Definujte subsystém IBM MQ na z/OS” na stránce 807.
2. Změňte hodnotu IEASYSpp tak, aby při provádění IPL byly použity následující členy:

- členy PROGxx nebo IEAAPFaa použité v “Autorizace APF pro zaváděcí knihovny produktu IBM MQ” na stránce 802
- členy LNKLSTkk a LPALSTmm použité v produktu “Aktualizovat seznam odkazů z/OS a LPA” na stránce 803
- Člen SCHEDxx použitý v “Aktualizace tabulky vlastností programu z/OS” na stránce 807
- Člen IEFSSNss používaný v produktu “Definujte subsystém IBM MQ na z/OS” na stránce 807

Související pojmy

“Upravit vstupní datové sady inicializace” na stránce 815
Vytvořte pracovní kopie vstupních datových sad inicializace a upravte je tak, aby vyhovovala požadavkům vašeho systému.

z/OS *Upravit vstupní datové sady inicializace*

Vytvořte pracovní kopie vstupních datových sad inicializace a upravte je tak, aby vyhovovala požadavkům vašeho systému.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Při migraci z předchozí verze je třeba provést tuto úlohu.*

Každý správce front produktu IBM MQ získává počáteční definice ze série příkazů obsažených v *inicializačních vstupních datových sadách*produktu IBM MQ . Tyto datové sady jsou odkazovány pomocí názvů definic dat CSQINP1, CSQINP2 a CSQINPT definovaného v proceduře úlohy spuštěné správcem front.

Odezvy na tyto příkazy jsou zapsány do inicializačních výstupních datových sad, na které odkazují názvy definic dat CSQOUT1, CSQOUT2 a CSQOUTT.

Chcete-li zachovat originály, vytvořte pracovní kopie každého vzorku. Potom můžete upravit příkazy v těchto pracovních kopiích tak, aby odpovídaly požadavkům vašeho systému.

Pokud použijete více než jeden subsystém IBM MQ , pokud zahrnete název subsystému do kvalifikátoru vysoké úrovně názvu vstupní datové sady inicializace, můžete identifikovat subsystém IBM MQ přidružený ke každé datové sadě snadněji.

Další informace o ukázkách naleznete v následujících tématech:

- Formáty inicializačních datových sad
- Použití ukázky CSQINP1
- Použití ukázek CSQINP2
- Použití ukázky CSQINPX
- Použití ukázky CSQINPT

Formáty inicializačních datových sad

Vstupní datové sady inicializace mohou být členy rozdělené datové sady (PDS) nebo sekvenční datové sady. Mohou se jednat o zřetězenou řadu datových sad. Definujte je s délkou záznamu 80 bajtů, kde:

- Významné jsou pouze sloupce 1 až 72. Sloupce 73 až 80 se ignorují.
- Záznamy s hvězdičkou (*) ve sloupci 1 jsou interpretovány jako komentáře a jsou ignorovány.
- Prázdné záznamy se ignorují.
- Každý příkaz musí začínat na novém záznamu.
- Koncové-znamená pokračovat od sloupce 1 dalšího záznamu.
- Koncový znak + znamená pokračovat od prvního nemezerových sloupců dalšího záznamu.
- Maximální počet znaků povolených v příkazu je 32 762.

Výstupní datové sady inicializace jsou sekvenční datové sady, s délkou záznamu 125, formátem záznamu VBA a velikostí bloku 629.

Použití ukázky CSQINP1

Datová sada thlqual.SCSQPROC obsahuje dva členy, které obsahují definice fondů vyrovnávacích pamětí, sadu stránek do asociací fondů vyrovnávacích pamětí a příkaz ALTER SECURITY.

Člen CSQ4INP1 používá jednu stránku nastavenou pro každou třídu zprávy. Člen CSQ4INPR používá více sad stránek pro hlavní třídy zprávy.

Začleňte odpovídající vzorek do zřetězení CSQINP1 spuštěné procedury úlohy spuštěné správce front.

Notes:

1. IBM MQ podporuje až 100 vyrovnávacích pamětí v rozsahu 0 až 99. Příkaz DEFINE BUFFPOOL může být vydán pouze z inicializační datové sady CSQINP1 . Definice v ukázce uvádějí čtyři fondy vyrovnávacích pamětí.
2. Každá sada stránek použitá správcem front musí být definována v datové sadě inicializace CSQINP1 pomocí příkazu DEFINE PSID. Definice sady stránek přidružuje ID fondu vyrovnávacích pamětí k sadě stránek. Není-li určen žádný fond vyrovnávacích pamětí, je při výchozím nastavení použit nulový fond vyrovnávacích pamětí.

   Musí být definována kódová stránka nula (00). Obsahuje všechny definice objektů. Pro každého správce front lze definovat až 100 sad stránek.
3. Příkaz ALTER SECURITY lze použít ke změně atributů zabezpečení TIMEOUT a INTERVAL. V CSQ4INP1jsou výchozí hodnoty definovány jako 54 pro TIMEOUT a 12 pro INTERVAL.

Informace o uspořádání fondů vyrovnávacích pamětí a sad stránek naleznete v příručce Plánování na z/OS .

Pokud změníte fond vyrovnávacích pamětí a definice sad stránek dynamicky za běhu správce front, měli byste také aktualizovat definice CSQINP1 . Změny se zachovají pouze pro studený start produktu IBM MQ, pokud definice fondu vyrovnávacích pamětí neobsahuje atribut REPLACE.

Použití ukázek CSQINP2

Tato tabulka obsahuje seznam členů thlqual.SCSQPROC , které lze zahrnout do zřetězení CSQINP2 procedury spuštěné úlohy správce front spolu s popisem jejich funkce. Konvence pojmenování je CSQ4INS*. CSQ4INY* bude třeba upravit pro vaši konfiguraci. Měli byste se vyvarovat změny členů CSQINS*, protože budete muset znovu použít jakékoli změny, když migrujete na další vydání. Místo toho můžete vložit příkazy DEFINE nebo ALTER do členů CSQ4INY* .

Tabulka 57. Členové thlqual.SCSQPROC

Název člena	**Popis**
CSQ4INSG	Definice systémových objektů.
CSQ4INSA	Systémový objekt a výchozí pravidla pro ověření kanálu.
CSQ4INSX	Definice systémových objektů.
CSQ4INSS	Tento člen můžete upravit a zahrnout, pokud používáte skupiny sdílení front.
CSQ4INSJ	Tento člen upravte a začleňte, pokud používáte publikování/odběr pomocí produktu JMS.
CSQ4INSM	Definice systémových objektů pro Advanced Message Security.
CSQ4INSR	Upravte a zahrňte tento člen, pokud používáte produkt WebSphere Application Servernebo rozhraní publikování/odběru ve frontě podporované démonem publikování/odběru zařazeného ve frontě v produktu IBM MQ V7 nebo pozdější.

Tabulka 57. Členové thlqual.SCSQPROC (pokračování)	
Název člena	**Popis**
CSQ4DISP	Ukázka CSQINP2 pro zobrazení definic objektů.
CSQ4INYC	Definice klastrování.
CSQ4INYD	Distribuované definice front.
CSQ4INYG	Obecné definice.
CSQ4INYR	Definice tříd úložišť, použití více sad stránek pro hlavní třídy zprávy.
CSQ4INYS	Definice tříd úložišť pomocí jedné sady stránek pro každou třídu zprávy.

Musíte definovat objekty pouze jednou, ne vždy, když spustíte správce front, takže není nutné tyto definice zahrnout do CSQINP2 pokaždé. Pokud je zahrnete pokaždé, pokoušíte se definovat objekty, které již existují, a budete mít podobné zprávy jako následující:

```
CSQM095I +CSQ1 CSQMAQLC QLOCAL(SYSTEM.DEFAULT.LOCAL.QUEUE) ALREADY EXISTS
CSQM090E +CSQ1 CSQMAQLC FAILURE REASON CODE X'00D44003'
CSQ9023E +CSQ1 CSQMAQLC ' DEFINE QLOCAL' ABNORMAL COMPLETION
```

Tyto objekty nejsou poškozeny tímto selháním. Chcete-li ponechat datovou sadu definic SYSTEM v zřetězení CSQINP2 , můžete se vyhnout zprávám o selhání tím, že uvedete atribut REPLACE pro každý objekt.

Použití vzorku CSQINPX

Ukázka thlqual.SCSQPROC(CSQ4INPX) obsahuje sadu příkazů, které byste mohli chtít provést při každém spuštění inicializátoru kanálu. Jedná se obvykle o příkazy související s kanály, jako je například START LISTENER, které se požadují při každém spuštění inicializátoru kanálu, nikoli vždy při spuštění správce front a které nejsou povoleny ve vstupních datových sadách CSQINP1 nebo CSQINP2. Tuto ukázku si musíte před použitím upravit; můžete ji pak zahrnout do datové sady CSQINPX pro iniciátor kanálu.

Příkazy IBM MQ obsažené v datové sadě jsou prováděny na konci inicializace inicializátoru kanálu a výstup se zapisuje do datové sady určené příkazem CSQOUTX DD. Výstup je podobný výstupu, který je vytvořen funkcí COMMAND obslužného programu IBM MQ (CSQUTIL). Další podrobnosti najdete v tématu Obslužný program CSQUTIL .

Můžete zadat kterýkoli z příkazů IBM MQ , které lze vydat z CSQUTIL, nikoli pouze příkazy kanálu. Můžete zadávat příkazy z jiných zdrojů, zatímco je CSQINPX zpracováván. Všechny příkazy jsou vydávány v pořadí bez ohledu na úspěch předchozího příkazu.

Chcete-li určit dobu odezvy příkazu, můžete použít příkaz pseudo-command jako první příkaz v datové sadě. To trvá jedno volitelné klíčové slovo RESPTIME (*nnn*), kde *nnn* je doba čekání na odpověď na každý příkaz, v sekundách. To je v rozsahu od 5 do 999; předvolba je 30.

Pokud IBM MQ zjistí, že odpovědi na čtyři příkazy zabraly příliš dlouho, zpracování CSQINPX je zastaveno a žádné další příkazy nejsou vydány. Inicializátor kanálu není zastaven, ale zpráva CSQU052E je zapsána do datové sady CSQOUTX a zpráva CSQU013E je odeslána na konzolu.

Když produkt IBM MQ úspěšně dokončil zpracování objektu CSQINPX, odešle se na konzolu zpráva CSQU012I .

Použití ukázky CSQINPT

Tato tabulka obsahuje seznam členů thlqual.SCSQPROC , které lze zahrnout do zřetězení CSQINPT u procedury spuštěné úlohy správce front, s popisem jejich funkce.

Tabulka 58. Členové thlqual.SCSQPROC	
Název člena	**Popis**
CSQ4INST	Výchozí definice odběru systému.
CSQ4INYT	Definice publikování/odběru.

Příkazy IBM MQ obsažené v datové sadě jsou provedeny při dokončení inicializace publikování/odběru a výstup je zapisován do datové sady určené příkazem CSQOUTT DD. Výstup je podobný výstupu, který je vytvořen funkcí COMMAND obslužného programu IBM MQ (CSQUTIL). Další podrobnosti najdete v tématu Obslužný program CSQUTIL .

Související pojmy

"Vytvoření zaváděcího programu a datových sad protokolu" na stránce 818
Pomocí dodaného programu CSQJU003 připravte zaváděcí datové sady (BSDSs) a datové sady protokolů.

z/OS *Vytvoření zaváděcího programu a datových sad protokolu*

Pomocí dodaného programu CSQJU003 připravte zaváděcí datové sady (BSDSs) a datové sady protokolů.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- V 9.1.4 *Pokud používáte šifrování datové sady produktu z/OS k ochraně BSDS nebo aktivních datových sad protokolů, je třeba tuto volbu konfigurovat před přiděleným datovým sadám v tomto kroku.*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*

  V 9.1.4 *Pokud provádíte migraci správce front a přidáváte-li šifrování datové sady produktu z/OS pro aktivní datové sady žurnálu nebo BSDS, je třeba převést datové sady.*

  V 9.1.4 *Viz část* důvěrnost dat ve zbytku produktu IBM MQ for z/OS s šifrováním datové sady. *Další informace o konfiguraci šifrování datové sady produktu z/OS a převodu existujících datových sad produktu IBM MQ na šifrovaně.*

Ukázkové řídicí příkazy jazyka JCL a služby Access Method (AMS) ke spuštění CSQJU003 pro vytvoření jednoho nebo duálního prostředí protokolování se budou konat v souboru thlqual.SCSQPROC(CSQ4BSDS). Upravte a spusťte tuto úlohu, abyste vytvořili BSDS a protokoly a předformátujte protokoly.

Důležité: Měli byste použít nejnovější verzi souboru CSQ4BSDSnebo aktualizovat JCL ručně pro použití RECORDS (850 60).

Procedura spuštěné úlohy, CSQ4MSTR, popsaná v tématu "Vytvoření procedur pro správce front produktu IBM MQ" na stránce 811, odkazuje na BSDSs v příkazech ve tvaru:

```
//BSDS1   DD DSN=++HLQ++.BSDS01,DISP=SHR
//BSDS2   DD DSN=++HLQ++.BSDS02,DISP=SHR
```

Na datové sady protokolu odkazuje BSDSs.

Poznámka:

1. Příkaz BLKSIZE musí být zadán v příkazu SYSPRINT DD v kroku LOGDEF. Hodnota BLKSIZE musí být 629.
2. Chcete-li usnadnit identifikaci sad dat pro samozavedení a datových sad protokolů z různých správců front, začleňte název subsystému do kvalifikátoru vyšší úrovně těchto datových sad.
3. Používáte-li skupiny sdílení front, musíte definovat zaváděcí program a datové sady protokolu s hodnotou SHAREOPTIONS (2 3).

Chcete-li získat informace o plánování zaváděcího programu a datových sad protokolů a jejich velikosti, prohlédněte si příručku Plánování na z/OS .

Rozšíření protokolu RBA protokolu o velikosti 8 bajtů z produktu IBM MQ 8.0zlepšuje dostupnost správce front, jak je popsáno v tématu Větší relativní adresa bajtů protokolu. Chcete-li před prvním spuštěním správce front povolit osmibajtovou adresu RBA protokolu, proveďte po vytvoření svého prostředí protokolování následující kroky.

1. Pomocí **IDCAMS ALTER**přejmenujte formát BSDSs formátu verze 1 (vytvořený pomocí programu CSQJU003) k něčemu jako ++HLQ++.V1.BSDS01.

   Poznámka: Ujistěte se, že jste přejmenovali komponenty dat a indexu stejně jako klastr VSAM.
2. Přidělte nové BSDS se stejnými atributy jako ty, které již byly definovány. Tato hodnota se stane formátem BSDSs formátu verze 2, který bude použit správcem front při jeho spuštění.
3. Spusťte obslužný program převodu BSDS (CSQJUCNV) pro převod sady BSD verze 1 na novou verzi BSDSs formátu 2.
4. Jakmile je konverze úspěšně dokončena, odstraňte BSDSs formátu verze 1.

Poznámka: V 9.1.0 Je-li správce front ve skupině sdílení front, musí být všechny správce front v této skupině sdílení front spuštěny dříve, než bude povolen 8 bajtů protokolu RBA protokolu:

- Je-li správce front v IBM MQ 8.0.0 , musí být spuštěn s **OPMODE**(*NEWFUNC,800*)
- Je-li správce front v IBM MQ 9.0.0 LTS , musí být spuštěn s **OPMODE**(NEWFUNC,900) nebo **OPMODE**(*NEWFUNC,800*).
- Je-li správce front v IBM MQ 9.0.n CD, IBM MQ 9.1.0 LTSnebo pozdější, musí být spuštěn na této úrovni

Související pojmy

“Definujte sady stránek” na stránce 819
Nadefinujte sady stránek pro každého správce front pomocí jednoho z dodaných ukázek.

z/OS *Definujte sady stránek*

Nadefinujte sady stránek pro každého správce front pomocí jednoho z dodaných ukázek.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ .*

  V 9.1.4 *Pokud používáte šifrování datové sady produktu z/OS k ochraně sad stránek, je třeba tuto volbu konfigurovat před přiděleným datovým sadám v tomto kroku.*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*

  V 9.1.4 *Pokud migrujete správce front a přidáváte šifrování datové sady produktu z/OS pro sady stránek, je třeba převést sady stránek.*

  V 9.1.4 *Viz část* důvěrnost dat ve zbytku produktu IBM MQ for z/OS s šifrováním datové sady. *Další informace o konfiguraci šifrování datové sady produktu z/OS a převodu existujících datových sad produktu IBM MQ na šifrovaně.*

Definujte oddělené sady stránek pro každého správce front IBM MQ . Soubory thlqual.SCSQPROC(CSQ4PAGE) a thlqual.SCSQPROC(CSQ4PAGR) obsahují příkazy řízení a formátování sad stránek aplikací (AMS) jazyka JCL a produktu z/OS (DB2). Člen CSQ4PAGE používá jednu sadu stránek pro každou třídu zprávy, člen CSQ4PAGR používá více sad stránek pro hlavní třídy zprávy. JCL spouští dodaný obslužný program CSQUTIL. Přezkoumejte ukázky a upravte je podle počtu sad stránek, které chcete, a velikosti, které se mají použít. Informace o sadách stránek a o tom, jak vypočítat vhodné velikosti, naleznete v příručce Plánování na z/OS .

Procedura spuštěné úlohy CSQ4MSTR popsaná v “Vytvoření procedur pro správce front produktu IBM MQ” na stránce 811 odkazuje na sady stránek, v příkazu ve tvaru:

```
//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. Hodláte-li používat funkci rozšíření dynamické sady stránek, ujistěte se, že jsou pro každou sadu stránek definovány sekundární fyzické oblasti. thlqual.SCSQPROC(CSQ4PAGE) ukazuje, jak to provést.
2. Chcete-li pomoci identifikovat sady stránek z různých správců front, zahrňte název subsystému do kvalifikátoru vyšší úrovně datové sady přidružené ke každé sadě stránek.
3. Pokud chcete povolit volbu FORCE, která má být použita spolu s funkcí FORMAT obslužného programu CSQUTIL, musíte přidat atribut REUSE na příkaz AMS DEFINE CLUSTER. Tento popis je popsán v publikaci Administrace IBM MQ for z/OS.
4. Pokud mají být vaše sady stránek větší než 4 GB, musíte použít funkci EXTENDED ADDRESABILITY systému SMS (Storage Management System).

Související pojmy

"Přidejte položky IBM MQ do tabulek Db2 ." na stránce 851
Používáte-li skupiny sdílení front, spusťte obslužný program CSQ5PQSG pro přidání skupin sdílení front a položek správce front do tabulek IBM MQ ve skupině sdílení dat produktu Db2 .

z/OS *Přizpůsobte modul systémových parametrů.*

Modul parametrů systému IBM MQ řídí prostředí protokolování, archivace, trasování a připojení, které IBM MQ používá při své operaci. Je dodán výchozí modul. Měli byste vytvořit svůj vlastní modul parametrů systému, protože některé parametry, například názvy datových sad, jsou obvykle specifické pro organizační jednotku.

- *Podle potřeby opakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu. Podrobné informace naleznete v tématu* Migrace produktu IBM MQ v systému z/OS*.*
- *Chcete-li povolit produkt Advanced Message Security for z/OS v existujícím správci front, stačí nastavit parametr SPLCAP na hodnotu YES, jak je popsáno v tématu* "Použití CSQ6SYSP" na stránce 822*. Pokud konfigurujete tohoto správce front poprvé, dokončete celou tuto úlohu.*

Modul parametrů systému má následující makra V 9.1.0 čtyři :

Název makra	Účel
CSQ6SYSP	Určuje parametry připojení a trasování, viz "Použití CSQ6SYSP" na stránce 822 .
CSQ6LOGP	Ovládá inicializaci protokolu, viz "Použití CSQ6LOGP" na stránce 831
CSQ6ARVP	Řídí inicializaci archivu, viz "Použití CSQ6ARVP" na stránce 835
V 9.1.0 V 9.1.0 CSQ6USGP	Ovládá záznam použití, viz "Použití CSQ6USGP" na stránce 842

Produkt IBM MQ dodává výchozí modul parametrů systému CSQZPARM, který je vyvolán automaticky, pokud zadáte příkaz START QMGR (bez parametru PARM) ke spuštění instance produktu IBM MQ. CSQZPARM je v knihovně autorizace APF thlqual.SCSQAUTH také dodána s IBM MQ. Hodnoty těchto parametrů se zobrazí jako série zpráv, když spustíte IBM MQ.

Další informace o použití tohoto příkazu najdete v části START QMGR .

Vytvoření vlastního modulu parametrů systému

Pokud CSQZPARM neobsahuje požadované systémové parametry, můžete vytvořit svůj vlastní modul parametrů systému pomocí vzorového souboru JCL uvedeného v souboru thlqual.SCSQPROC(CSQ4ZPRM).

Chcete-li vytvořit vlastní modul parametrů systému, postupujte takto:

1. Vytvořte pracovní kopii ukázky JCL.
2. Upravte parametry pro každé makro v kopii podle potřeby. Pokud odeberete všechny parametry z volání makra, výchozí hodnoty se automaticky vyzvednou za běhu.
3. Nahraďte zástupný symbol ++NAME++ názvem, který má načíst zaváděcí modul (tento může být CSQZPARM).
4. Pokud váš asembler není assembler vysoké úrovně, změňte kód JCL podle požadavků vašeho asembleru.
5. Spuštěním skriptu JCL sestavte a propojte úpravy upravených verzí maker systémových parametrů tak, aby vytvářeli modul načítání. Jedná se o nový modul parametrů systému s názvem, který jste zadali.
6. Vložte zaváděcí modul vytvořený v uživatelské knihovně s oprávněním APF.
7. Přidejte uživatelský přístup pro čtení k uživatelské knihovně oprávněných uživatelů APF.
8. Zahrňte tuto knihovnu do procedury úlohy STEPLIB pro spuštěnou úlohu správce front produktu IBM MQ . Tento název knihovny musí být uveden před knihovnou thlqual.SCSQAUTH v knihovně STEPLIB.
9. Při spuštění správce front vyvolejte nový modul parametrů systému. Je-li například nový modul pojmenován NEWMODS, zadejte následující příkaz:

   ```
   START QMGR PARM(NEWMODS)
   ```

10. Ujistěte se o úspěšném dokončení příkazu kontrolou protokolu úlohy. Záznam by měl být v protokolu podobný následujícímu:

    ```
    CSQ9022I CDL1 CSQYASCP 'START QMGR' NORMAL COMPLETION
    ```

Můžete také zadat název modulu parametrů ve spouštěcím skriptu JCL správce front. Další informace naleznete v tématu Spuštění a zastavení správce front.

Poznámka: Pokud si zvolíte pojmenování svého modulu CSQZPARM, nemusíte uvádět parametr PARM v příkazu START QMGR.

Podrobné vyladění modulu parametrů systému

Produkt IBM MQ také dodává sadu tří zdrojových modulů asembleru, které lze použít k dokončení vyladění existujícího modulu parametrů systému. Tyto moduly jsou v knihovně thlqual.SCSQASMS. Tyto moduly zpravidla použijete v testovacím prostředí ke změně výchozích parametrů v makrech parametrů systému. Každý zdrojový modul volá jiné makro parametru systému:

Tento zdrojový modul assembler ...	Vyvolá toto makro ...
CSQFSYSP	CSQ6SYSP (parametry připojení a trasování)
CSQJLOGP	CSQ6LOGP (inicializace protokolu)
CSQJARVP	CSQ6ARVP (inicializace archivu)

Tímto způsobem můžete používat tyto moduly:

1. Vytvoření pracovních kopií každého modulu zdroje v asembleru v knihovně asembleru uživatele.
2. Upravte své kopie přidáním nebo změnou hodnot jakýchkoli parametrů podle potřeby.
3. Sestavte své kopie všech upravených modulů a vytvořte moduly objektů v knihovně uživatelských objektů.
4. Odkaz na úpravy těchto modulů kódu objektu s existujícím modulem parametrů systému za účelem vytvoření modulu zavedení, který je novým modulem parametrů systému.
5. Ujistěte se, že nový modul systémových parametrů je členem autorizované knihovny uživatele.

6. Zahrňte tuto knihovnu do procedury úlohy STEPLIB spuštěné úlohy správce front. Tato knihovna musí být uvedena před knihovnou thlqual.SCSQAUTH v knihovně STEPLIB.
7. Vyvolejte nový modul parametrů systému zadáním příkazu START QMGR, zadáním nového názvu modulu v parametru PARM, jako dříve.

Ukázkový usermod je poskytován ve členu CSQ4UZPR SCSQPROC, který demonstruje, jak spravovat upravené systémové parametry pod kontrolou SMP/E.

Změna systémových parametrů

Při spuštění správce front můžete změnit některé systémové parametry. Informace o příkazech SET SYSTEM, SET LOGa SET ARCHIVE naleznete v následujících příkazech.

Vložení příkazů SET do vstupních datových sad inicializace tak, aby nabyly účinnosti při každém spuštění správce front.

Související pojmy

“Přizpůsobte parametry inicializátoru kanálu” na stránce 843
Pomocí příkazu ALTER QMGR můžete upravit inicializátor kanálu tak, aby vyhovoval vašim požadavkům.

z/OS *Použití CSQ6SYSP*

Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6SYSP.

Výchozí parametry pro CSQ6SYSPa to, zda můžete změnit jednotlivé parametry pomocí příkazu SET SYSTEM, jsou zobrazeny v Tabulka 59 na stránce 822. Chcete-li některou z těchto hodnot změnit, přečtěte si podrobné popisy parametrů.

Tabulka 59. Výchozí hodnoty parametrů CSQ6SYSP

Parametr	Popis	Výchozí hodnota	příkaz SET
ACELIM	Velikost fondu úložišť ACE v blocích o velikosti 1 KB.	0 (bez omezení)	✓
CLCACHE	Určuje typ mezipaměti klastru, který má být použit.	STATICKÝ	-
CMDUSER	Výchozí ID uživatele pro kontroly zabezpečení příkazů.	CSQOPR	-
EXCLMSG	Uvádí seznam zpráv, které mají být vyloučeny z jakéhokoli protokolu. Zprávy v tomto seznamu se neodešlou do konzoly z/OS a do protokolu hardcopy. Výsledkem použití parametru EXCLMSG k vyloučení zpráv je efektivnější z perspektivy CPU než použití metod popsaných v “Potlačit informační zprávy” na stránce 847	( )	✓
EXITLIM	Doba (v sekundách), po kterou mohou být uživatelské procedury správců front spuštěny během každého vyvolání.	30	-
EXITTCB	Počet spuštěných úloh serveru, které mají být použity ke spuštění správce front.	8	-
LOGLOAD	Počet záznamů protokolu zapsaných pomocí IBM MQ mezi začátkem jednoho kontrolního bodu a dalším.	500 000	✓

Tabulka 59. Výchozí hodnoty parametrů CSQ6SYSP (pokračování)			
Parametr	**Popis**	**Výchozí hodnota**	**příkaz SET**
MULCCAPT	Určuje vlastnost Naměřená cena využití, která řídí algoritmus pro shromažďování dat používaných měřenými licenčními poplatky za použití (MULC).	Viz popis parametru	-
OTMACON	Parametry připojení OTMA.	Viz popis parametru	-
QINDXBLD	Určuje, zda bude restartování správce front čekat, než budou všechny indexy znovu sestaveny nebo budou dokončena před přestavením všech indexů.	WAIT	-
QMCCSID	Identifikátor kódované znakové sady pro správce front.	Nula	-
QSGDATA	Parametry skupiny sdílení front.	Viz popis parametru	-
RESAUDIT	parametr monitorování RESLEVEL.	YES	-
ROUTCDE	Směrovací kód zprávy přiřazený zprávám, které nejsou vyžádané z určité konzoly.	1	-
SERVICE	Rezervováno pro použití produktem IBM.	0	✓
SMFACCT	Určuje, zda mají být shromažďována data evidence SMF při spuštění správce front. Všimněte si, že data evidence kanálu třídy 4 jsou shromažďována pouze v případě, že je spuštěn inicializátor kanálu.	NO	-
SMFSTAT	Určuje, zda má být shromažďována statistika SMF při spuštění správce front. Všimněte si, že statistická data o inicializátoru kanálu třídy 4 jsou shromažďována pouze v případě, že je spuštěn inicializátor kanálu.	NO	-
SPLCAP	Určuje, zda je v tomto správci front povolena funkce zásad zabezpečení fronty. U parametru Advanced Message Security for z/OSnastavte tento parametr na hodnotu YES.	NO	-
STATIME	Výchozí čas, v minutách, mezi každým shromážděním statistických údajů.	30	✓
TRACSTR	Určuje, zda má být trasování spuštěno automaticky.	NO	-
TRACTBL	Velikost trasovací tabulky v blocích o velikosti 4 KB, která má být použita prostředkem globálního trasování.	99 (396 KB)	✓
WLMTIME	Doba mezi skenováním indexu fronty pro fronty spravované WLM.	30	-
WLMTIMU	Jednotky (minuty nebo sekundy) pro operaci WLMTIME.	minuty	-

ACELIM

Určuje maximální velikost fondu úložišť ACE v 1kB blocích. Číslo musí být v rozsahu 0-999999. Výchozí hodnota nula znamená, že nejsou určena žádná omezení nad rámec možností systému.

Hodnotu ACELIM byste měli nastavit pouze pro správce front, u nichž bylo zjištěno nadměrné používání úložiště ECSA. Omezení fondu úložišť ACE je limitováno počtem připojení v systému, a tedy množstvím úložiště ECSA používané správcem front.

Jakmile správce front dosáhne limitu, není možné pro aplikace získat nová připojení. Nedostatek nových připojení způsobí selhání ve zpracování MQCONN a u aplikací koordinovaných prostřednictvím služby RRS bude pravděpodobně docházet k selháním v nějakém 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); jsou to první dva společně přidané prvky v QSRSPHBT.

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.

CCACHE

Určuje typ mezipaměti klastru, který má být použit.

Mezipaměť klastru je oblast úložiště, která se používá k ukládání informací souvisejících s klastrem.

Je-li mezipaměť klastru statická, bude mít pevnou velikost, která je přidělena při spuštění správce front. Pokud se mezipaměť zaplní, pak se vydá zpráva CSQM060E a požadavek aplikace, který vyžaduje více prostoru, obdrží chybu MQRC_CLUSTER_RESOURCE_ERROR.

Nastavíte-li CLCACHE na dynamickou, může se mezipaměť klastru podle potřeby rozšířit. Nejprve je však třeba zajistit, aby všechny instalované uživatelské procedury pracovní zátěže klastru mohly fungovat s dynamickou mezipamětí.

Pokud nainstalovaná uživatelská procedura pracovní zátěže klastru nemůže fungovat se zprávou dynamické mezipaměti CSQM061E , bude vydána.

MQXCLWLNje poskytnut pro pracovní zátěž klastru, která slouží k navigaci v mezipaměti klastru způsobem, který funguje bez ohledu na to, zda jsou použity dynamické nebo statické mezipaměti.

Pro nové správce front nastavte CLCACHE=DYNAMIC, pokud nechystáte se použít uživatelskou proceduru pracovní zátěže klastru, která nepodporuje dynamickou mezipaměť.

Pro existující správce front, kteří již používají statickou mezipaměť a nacházejí se v klastru, který nemá mnoho nových front a správců front k němu přidáno, je vhodné pokračovat s použitím STATCACHIC CLCACHE=STATIC.

Pro stávající správce front, kteří již používají statickou mezipaměť a jsou v klastru, k nimž se přidá mnoho nových front nebo správců front, začněte používat CLCACHE=DYNAMIC.

STATICKÝ

Je-li mezipaměť klastru statická, její velikost je pevně daná při spuštění správce front, což je dostatečné pro aktuální množství informací o klastru a navíc i prostor pro rozšíření. Velikost nelze zvýšit, je-li správce front aktivní. Toto nastavení je výchozí.

DYNAMICKÝ

Je-li mezipaměť klastru dynamická, počáteční velikost alokovaná při spuštění správce front může být automaticky zvýšena, je-li to nutné, zatímco je správce front aktivní.

CMDUSER
Uvádí výchozí ID uživatele použité pro kontroly zabezpečení příkazu. Toto ID uživatele musí být definováno pro ESM (například RACF). Zadejte název o délce 1 až 8 alfanumerických znaků. První znak musí být písmeno.

Předvolba je CSQOPR.

EXCLMSG
Uvádí seznam chybových zpráv, které mají být vyloučeny.

Tento seznam je dynamický a je aktualizován pomocí příkazu SET SYSTEM.

Výchozí hodnota je prázdný seznam ().

Zprávy se dodávají bez předpony CSQ a bez přípony kódu akce (I-D-E-A). Chcete-li například vyloučit zprávu CSQX500I, přidejte X500 do tohoto seznamu. Tento seznam může obsahovat maximálně 16 identifikátorů zpráv.

Aby mohla být tato zpráva zařazena do seznamu, musí být vydána po normálním spuštění adresních prostorů MSTR nebo CHIN a začínat jedním z následujících znaků E, H, I, J, L, M, N, P, R, T, V, W, X, Y, 2, 3, 5, 9.

Identifikátory zpráv, které jsou vydány jako výsledek zpracování příkazů, mohou být přidány do seznamu, avšak nebudou vyloučeny. Například, identifikátor zprávy je vydán jako výsledek příkazu DISPLAY USAGE PSID (*), tato zpráva však nemůže být potlačena.

EXITLIM
Určuje dobu (v sekundách) povolenou pro každé vyvolání správce front. (Tento parametr nemá žádný vliv na uživatelské procedury kanálu.)

Uveďte hodnotu v rozsahu 5 až 9999.

Výchozí hodnota je 30. Správce front vyzývá procedury, které jsou spuštěny každých 30 sekund. U každého typu poll jsou všechny, které byly spuštěny déle, než je čas určený produktem EXITLIM, vynuceně ukončeni.

EXITTCB
Určuje počet spuštěných úloh serveru, které mají být použity ke spuštění uživatelských procedur ve správci front. (Tento parametr nemá žádný vliv na uživatelské procedury kanálu.) Musíte zadat číslo alespoň tak vysoké, jako je maximální počet uživatelských procedur (jiných než uživatelských procedur kanálu), které může správce front spustit, jinak dojde k selhání s abend 6c6 .

Uveďte hodnotu v rozsahu 0 až 99. Hodnota nula znamená, že žádné uživatelské procedury nelze spustit.

Výchozí hodnota je 8.

LOGLOAD
Uvádí počet záznamů protokolu, které IBM MQ zapisuje mezi začátkem jednoho kontrolního bodu a dalším. Produkt IBM MQ zahájí nový kontrolní bod po zapsání počtu záznamů, které zadáte.

Zadejte hodnotu v rozsahu 200 až 16 000 000.

Výchozí hodnota je 500 000.

Čím vyšší je hodnota, tím lepší je výkon produktu IBM MQ ; Nicméně restartování trvá déle, je-li parametr nastaven na velkou hodnotu.

Doporučené nastavení:

Testovací systém	10 000
Produkční systém	500 000 V produkčním systému může dodaná výchozí hodnota vést k příliš vysoké frekvenci kontrolních bodů.

Hodnota volby LOGLOAD určuje frekvenci kontrolních bodů správce front. Příliš velká hodnota znamená, že velké množství dat je zapsáno do protokolu mezi kontrolními body, což vede k vyššímu času restartování zotavení správce front, který následuje po selhání. Příliš nízká hodnota způsobuje, že se kontrolní body vyskytují příliš často při špičkovém zatížení, nepříznivě ovlivňují doby odezvy a využití procesoru.

Pro LOGLOAD je doporučována počáteční hodnota 500 000. Pro četnost trvalých zpráv 1 kB 100 zpráv za sekundu (tj. 100 příkazů `MQPUT` s potvrzením a 100 `MQGET` s potvrzováním) je interval mezi kontrolními body přibližně 5 minut.

Poznámka: To je určeno pouze jako vodítko a optimální hodnota pro tento parametr je závislá na charakteristikách jednotlivých systémů.

MULCCAPT
Určuje algoritmus, který má být použit pro shromažďování dat používaných měřenými licenčními poplatky za použití (MULC).

STANDARD
MULTC je založen na čase volání MQCONN rozhraní API produktu IBM MQ na dobu volání MQDISC rozhraní API produktu IBM MQ .

Upřesněno
MULTC je založen na čase od začátku volání API IBM MQ na konec volání API IBM MQ .

Výchozí hodnota je STANDARD.

OMMAKON
Parametry OTMA. Toto klíčové slovo má pět pozičních parametrů::

OTMACON = (`Group,Member,Druexit,Age,Tpipepfx`)

Skupina
Jedná se o název skupiny XCF, do které patří tato konkrétní instance produktu IBM MQ .

Může být 1 až 8 znaků dlouhý a musí být zadán velkými písmeny.

Výchozí hodnota je prázdná, což znamená, že produkt IBM MQ se nesmí pokoušet o připojení ke skupině XCF.

Člen
Jedná se o název člena této konkrétní instance produktu IBM MQ ve skupině XCF.

Může být 1 až 16 znaků dlouhý a musí být zadán velkými písmeny.

Předvolba je 4znakový název správce front.

Druexit
Uvádí název uživatelské procedury rozpoznání cíle OTMA, která má být spuštěna produktem IMS.

Může mít délku 1 až 8 znaků.

Předvolba je DFSYDRU0.

Tento parametr je volitelný; je povinný, pokud má IBM MQ přijímat zprávy z aplikace IMS , která nebyla spuštěna produktem IBM MQ. Název musí odpovídat uživatelské proceduře rozpoznání místa určení, která je kódována v systému IMS . Další informace viz “Použití uživatelských procedur OTMA v adresáři IMS” na stránce 912.

Věk
Představuje dobu, v sekundách, po kterou je ID uživatele z produktu IBM MQ považováno za dříve ověřené IMS.

Může být v rozsahu nula až 2 147 483 647.

Výchozí hodnota je 2 147 483 647.

Doporučuje se nastavit tento parametr ve spojení s parametrem `interval` příkazu ALTER SECURITY tak, aby byla zachována konzistence nastavení mezipaměti zabezpečení v rámci sálového počítače.

Tpipepfx
To představuje předponu, která se má použít pro názvy Tpipe.

Skládá se ze tří znaků; první znak je v rozsahu A až Z, následné znaky jsou A až Z nebo 0 až 9. Výchozí hodnota je CSQ.

Toto se použije pokaždé, když produkt IBM MQ vytvoří Tpipe; zbytek názvu je přiřazen pomocí IBM MQ. Nelze nastavit úplný název Tpipe pro všechny nástroje Tpipe vytvořené produktem IBM MQ.

QINDXBLD
Určuje, zda bude restartování správce front čekat, dokud nebudou všechny indexy fronty znovu sestaveny nebo budou pokračovat, než budou znovu sestaveny všechny indexy.

WAIT
Restartování správce front čeká na dokončení všech sestavení indexu fronty. To znamená, že během normálního zpracování rozhraní API produktu IBM MQ během vytváření indexu nejsou zpožděny žádné aplikace, protože všechny indexy jsou vytvořeny dříve, než se mohou k tomuto správci front připojit všechny aplikace.

Toto nastavení je výchozí.

NoWait
Správce front lze restartovat, než bude dokončena veškerá sestavení indexu fronty.

QMCCSID
Určuje výchozí identifikátor kódované znakové sady, který má správce front (a tedy i distribuované fronty) používat.

Uveďte hodnotu v rozsahu nula až 65535. Hodnota musí představovat kódovou stránku EBCDIC uvedenou jako nativní kódovou stránku z/OS pro zvolený jazyk v národních jazycích.

Nula, což je předvolená hodnota, znamená použít CCSID momentálně nastavený, nebo, pokud žádný není nastaven, použijte CCSID 500. To znamená, že pokud jste explicitně nastavili hodnotu CCSID na jakoukoli jinou než nulovou hodnotu, nemůžete ji resetovat nastavením hodnoty QMCCSID na nulu; nyní musíte použít správný nenulový CCSID. Je-li QMCCSID nula, můžete zkontrolovat, jaké CCSID se skutečně používá, vydáním příkazu DISPLAY QMGR CCSID.

QSGDATA
Data skupiny sdílení front. Toto klíčové slovo má pět pozičních parametrů:

QSGDATA = (`Qsgname,Dsgname,Db2name,Db2serv ,Db2blob`)

QSGNAME
Jedná se o název skupiny sdílení front, do níž patří správce front.

Platné znaky naleznete v tématu Pravidla pojmenování objektů IBM MQ . Název:

- Může mít délku 1 až 4 znaky.
- Nesmí začínat číslicí
- Nesmí končit znakem @.

  Důvodem je to, že z důvodů implementace jsou názvy méně než čtyř znaků doplněny interně znaky @ symbolům,

Výchozí hodnotou je prázdné místo, které indikuje, že správce front není členem žádné skupiny sdílení front.

Dsgname
Jedná se o název skupiny sdílení dat produktu Db2 , ke které se má správce front připojit.

Může být 1 až 8 znaků dlouhý a musí být zadán velkými písmeny.

Výchozí hodnotou je prázdná místa, která označuje, že nepoužíváte skupiny sdílení front.

Db2name
Jedná se o název subsystému Db2 nebo připojení skupiny, ke kterému se má správce front připojit.

Může být 1 až 4 znaky dlouhé a musí být zadáno velkými písmeny.

Výchozí hodnotou je prázdná místa, která označuje, že nepoužíváte skupiny sdílení front.

Poznámka: Subsystém Db2 (nebo příloha skupiny) musí být ve skupině sdílení dat Db2 zadané v produktu `Dsgname`a všichni správci front musí určovat stejnou skupinu sdílení dat produktu Db2 .

Db2serv
Jedná se o počet úloh serveru použitých pro přístup k produktu Db2.

Může být v rozsahu od 4 do 10.

Výchozí hodnota je 4.

Db2blob
Jedná se o počet úloh produktu Db2 použitých pro přístup k binárním objektům BLOB (Binary Large Objects).

Může být v rozsahu od 4 do 10.

Výchozí hodnota je 4.

Uvedete-li jeden z parametrů názvu (tj. **Qsgname**, **Dsgname**nebo **Db2name**), musíte zadat hodnoty pro ostatní názvy, jinak IBM MQ selže.

RESAUDIT
Uvádí, zda jsou záznamy auditu RACF zapsány pro kontroly zabezpečení RESLEVEL prováděné během zpracování připojení.

Zadejte jednu z následujících možností:

NO
Monitorování RESLEVEL se neprovádí.

YES
Auditování RESLEVEL se provádí.

Výchozí hodnota je ANO.

ROUTCDE
Určuje výchozí směrovací kód zprávy produktu z/OS přiřazený zprávám, které nejsou odesílány v přímé odpovědi na příkaz MQSC.

Zadejte jednu z následujících možností:

1. Hodnota v rozsahu od 1 do 16 včetně.
2. Seznam hodnot oddělených čárkou a uzavřený v závorkách. Každá hodnota musí být v rozsahu od 1 do 16 včetně.

Výchozí hodnota je 1.

Další informace o kódech směrování příkazu z/OS naleznete v části *Popis zprávy* v jednom ze svazků v příručce *z/OS MVS Routing and Descriptor Codes* .

SERVICE
Toto pole je vyhrazeno pro použití produktem IBM.

SMFACCT
Určuje, zda produkt IBM MQ odesílá data evidence do prostředí SMF automaticky při spuštění správce front.

Zadejte jednu z následujících možností:

NO
Nezahajujte automatické shromažďování účetních dat.

YES
Spustit shromažďování dat evidence automaticky pro výchozí třídu 1.

celá čísla
Seznam tříd, pro které se evidence shromažďuje automaticky v rozsahu 1 až 4.

Výchozí hodnota je NO.

SMFSTAT
Určuje, zda mají být shromažďovány statistické údaje SMF automaticky při spuštění správce front.

Zadejte jednu z následujících možností:

NO
Nezahajujte automaticky shromažďování statistických údajů.

YES
Automaticky zahájit shromažďování statistiky pro výchozí třídu 1.

celá čísla
Seznam tříd, pro které se statistiky shromažďují automaticky v rozsahu od 1 do 4. Chcete-li shromažďovat statistiky třídy 2 nebo 3, musí být zadána také třída 1.

Výchozí hodnota je NO.

SPLCAP
Schopnost zásad zabezpečení umožňuje vyšší úroveň zabezpečení zpráv prostřednictvím zásad, které řídí, zda jsou zprávy podepisovány nebo šifrovány, jak jsou napsány a čteny z front.

Zpracování zásad zabezpečení je pro tohoto správce front povoleno konfigurací funkce SPLCAP s některou z následujících hodnot:

NO
Možnost implementace zásad zabezpečení zpráv pro fronty není povolena během inicializace správce front.

YES

Schopnosti zabezpečení zpráv jsou povoleny během inicializace správce front.

Je-li tento ovládací prvek nastaven, správce front se během inicializace pokusí načíst modul povolující licenci ze souboru SDRQAUTH a spustit další adresní prostor (AMSM).

Správce front se nespustí, pokud je licence AMS licencována a že je v místě nutná konfigurace zabezpečení zpráv.


Je-li správce front spuštěn v produktu IBM MQ 9.1.2 nebo dřívější, je třeba zkontrolovat, zda je knihovna SDRQAUTH součástí knihovny STEPLIB správce front a obsahuje modul povolení produktu AMS .

Pokud je správce front spuštěn v produktu IBM MQ 9.1.3 nebo později, zkontroluje, že je atribut AMSPROD nastaven na jeden z AMS, ADVANCED nebo ADVANCEDVUE.

Pokud jsou tyto kontroly úspěšné, jsou během inicializace správce front povoleny funkce zabezpečení zpráv a je spuštěn adresní prostor AMSM.

Pokud tyto kontroly selžou, nebo je-li na místě zabezpečení zpráv, správce front se nespustí.

Výchozí hodnota je NO.

STATIME
Určuje výchozí dobu (v minutách) mezi po sobě jdoucími shromažďováními statistických údajů.

Uveďte číslo v rozsahu 0 až 1440.

Pokud zadáte hodnotu nula, jsou statistická data i data evidence shromažďována v plošné zprávě shromažďování dat SMF. Informace o nastavení této funkce najdete v tématu Použití nástroje pro správu systému .

Výchozí hodnota je 30.

TRACSTR
Uvádí, zda se má globální trasování spustit automaticky.

Zadejte jednu z následujících možností:

NO
Nespouštět globální trasování automaticky.

YES
Spustí globální trasování automaticky pro výchozí třídu, třídu 1.

celá čísla
Seznam tříd, pro které má být globální trasování spuštěno automaticky v rozsahu od 1 do 4.

*****
Automaticky spustit globální trasování pro všechny třídy.

Výchozí hodnota je NO, pokud v makru nezadáte klíčové slovo.

Poznámka: Dodaný výchozí zaváděcí modul parametru systému (CSQZPARM) má TRACTSTR=YES (nastaveno v modulu asembleru CSQFSYSP). Pokud nechcete automaticky spustit trasování, buď vytvořte svůj vlastní modul parametrů systému, nebo vydejte příkaz STOP TRACE poté, co byl spuštěn správce front.

Podrobné informace o příkazu STOP TRACE naleznete v části STOP TRACE.

TRACTBL
Určuje výchozí velikost v blocích o velikosti 4 kB v tabulce trasování, kde prostředek globálního trasování ukládá trasovací záznamy IBM MQ .

Uveďte hodnotu v rozsahu od 1 do 999.

Výchozí hodnota je 99. To je ekvivalentní 396 KB.

Poznámka: Paměť pro trasovací tabulku je alokována v ECSA. Proto je třeba tuto hodnotu vybrat s opatrností.

WLMTIME
Určuje dobu (v minutách nebo sekundách, v závislosti na hodnotě WLMTIMU) mezi jednotlivými skenováním indexů ve frontách spravovaných pomocí WLM.

Uveďte hodnotu v rozsahu od 1 do 9999.

Výchozí hodnota je 30.

WLMTIMU
Časové jednotky použité s parametrem WLMTIME.

Zadejte jednu z následujících možností:

minuty
WLMTIME představuje počet minut.

s
WLMTIME představuje počet sekund.

Výchozí hodnota je MINS.

Související odkazy
“Použití CSQ6LOGP” na stránce 831
Toto téma použijte jako referenci, jak určit volby protokolování pomocí CSQ6LOGP.

“Použití CSQ6ARVP” na stránce 835
Toto téma slouží jako reference pro určení prostředí archivace pomocí CSQ6ARVP .

z/OS *Použití CSQ6LOGP*

Toto téma použijte jako referenci, jak určit volby protokolování pomocí CSQ6LOGP.

Použijte CSQ6LOGP k vytvoření voleb protokolování.

Výchozí parametry pro CSQ6LOGPa to, zda můžete změnit každý parametr pomocí příkazu SET LOG , jsou zobrazeny v Výchozí hodnoty parametrů CSQ6LOGP. Potřebujete-li změnit některou z těchto hodnot, přečtěte si podrobné popisy parametrů.

Tabulka 60. Výchozí hodnoty parametrů CSQ6LOGP

Parametr	Popis	Výchozí hodnota	příkaz SET
COMPLOG	Řídí, zda je komprese protokolu povolena.	NONE	X
DEALLCT	Doba, kdy archivní pásková jednotka zůstává nevyužita, než bude dealokována.	zero	X
INBUFF	Velikost úložiště vstupní vyrovnávací paměti pro aktivní a archivní datové sady žurnálu.	60 KB	-
MAXARCH	Maximální počet svazků protokolu archivace, které lze zaznamenat.	500	X
MAXCNOFF	Maximální počet úloh odlehčování CSQJOFF7 , které lze spustit paralelně.	31	-
MAXRTU	Maximální počet vyhrazených páskových jednotek alokovaných pro souběžné čtení páskových nosičů s protokolem archivace.	2	X
OFFLOAD	Archivování zapnuto nebo vypnuto.	ANO (ZAPNUTO)	-
OUTBUFF	Velikost úložiště výstupní vyrovnávací paměti pro aktivní a archivní datové sady žurnálu.	4 000 KB	-
TWOACTV	Jedno nebo duální aktivní protokolování.	ANO (duální)	-
TWOARCH	Jednoduché nebo duální protokolování archivace.	ANO (duální)	-
TWOBSDS	Jeden nebo dva BSDS.	ANO (duální BSDS)	-
WRTHRSH	Počet výstupních vyrovnávacích pamětí, které mají být vyplněny, než jsou zapsány do aktivních protokolových datových sad.	20	X
V 9.1.2 V 9.1.2 ZHYWRITE	Uvádí, zda je funkce zápisu zHyperpovolena.	NO	X

COMPLOG

Uvádí, zda je komprese protokolu povolena.

Uveďte buď:

NONE

Komprese protokolu není povolena.

RLE

Komprese protokolu je povolena za použití kódování run-length.

ANY
Správce front vybere kompresní algoritmus, který poskytuje největší stupeň komprese záznamu protokolu. Tato volba má za následek kompresi RLE.

Výchozí hodnota je NONE.

Další informace o kompresi protokolu viz Komprese protokolu.

DEALLCT
Uvádí dobu v minutách, po kterou může pásková jednotka pro čtení archivu zůstat nevyužita, než bude dealokována.

Uveďte jednu z následujících možností:

- Čas, v minutách, v rozsahu 0 až 1440
- NOLIMIT

Uvedením 1440 nebo NOLIMIT znamená, že pásková jednotka není nikdy dealokována.

Výchozí hodnota je nula.

Při čtení dat protokolu archivace z pásky se doporučuje nastavit tuto hodnotu dostatečně vysokou, aby umožňovala IBM MQ optimalizovat obsluhu pásek pro více aplikací čtení.

INBUFF
Uvádí velikost vstupní vyrovnávací paměti (v kilobajtech) pro čtení aktivních a archivních protokolů během obnovy. Použijte dekadické číslo v rozsahu 28 až 60. Uvedená hodnota je zaokrouhlena nahoru na násobek 4.

Výchozí hodnota je 60 kB.

Doporučené nastavení:

Testovací systém	28 KB
Produkční systém	60 KB Nastavte ji na maximum pro nejlepší výkon při čtení protokolu.

MAXARCH
Uvádí maximální počet svazků protokolu archivace, které lze zaznamenat v BSDS. Po překročení tohoto počtu začne záznam znovu na začátku BSDS.

Použijte dekadické číslo v rozsahu od 10 do 1000.

Výchozí hodnota je 500.

Doporučené nastavení:

Testovací systém	500 (výchozí)
Produkční systém	1 000 Nastavte toto na maximum tak, aby BSDS mohlo zaznamenávat tolik protokolů, kolik je možné.

Informace o protokolech a BSDS naleznete v tématu Správa prostředků produktu IBM MQ.

MAXCNOFF
Určuje počet úloh odlehčování CSQJOFF7 , které lze spustit paralelně.

To umožňuje vyladit správce front nebo správce front tak, že nebudou používat všechny dostupné páskové jednotky.

Místo toho správce front před pokusem o přidělení nových datových sad archivu vyčká, dokud nebude dokončena úloha odsunutí CSQJOFF7 .

Pokud správce front provádí archivaci na pásku, nastavte tento parametr tak, aby počet souběžných požadavků na pásku neměl být roven nebo větší než počet dostupných páskových jednotek, v opačném případě by systém mohl reagovat.

Mějte na paměti, že pokud se používá duální archivace, pak každá úloha odkládání provádí oba archivy, takže je třeba tento parametr nastavit odpovídajícím způsobem. Je-li například správce front dual archivovat na pásku, hodnota MAXCNOFF=2 umožní archivaci dvou aktivních protokolů souběžně se čtyřmi páskami.

Pokud několik správců front sdílí páskové jednotky, měli byste nastavit hodnotu MAXCNOFF pro každého správce front odpovídajícím způsobem.

Výchozí hodnota je 31.

Uveďte hodnotu v rozsahu od 1 do 31.

MAXRTU
Uvádí maximální počet vyhrazených páskových jednotek, které mohou být alokovány souběžně pro čtení páskových nosičů s protokolem archivace.

Tento parametr a parametr DEALLCT umožňují produktu IBM MQ optimalizovat čtení protokolu archivu z páskových zařízení.

Uveďte hodnotu v rozsahu od 1 do 99.

Výchozí nastavení je 2.

Doporučuje se, abyste nastavili hodnotu tak, aby byla alespoň o jeden menší než počet páskových jednotek, které jsou k dispozici pro produkt IBM MQ. Jinak byste mohli odložit proces odlehčování, což by mohlo ovlivnit výkon vašeho systému. Pro maximální propustnost při zpracování protokolu archivace určete největší možnou hodnotu této volby a nezapomeňte, že pro zpracování odkládání je třeba použít alespoň jednu páskovou jednotku.

OFFLOAD
Určuje, zda je archivace zapnuta nebo vypnuta.

Uveďte buď:

YES
Archivace je zapnuta

NO
Archivace je vypnutá

Výchozí hodnota je ANO.

Upozornění: Pokud pracujete v testovacím prostředí, vypněte archivaci produktu **ne** , pokud nepracujete. Pokud jej vypnete, nemůžete zaručit, že data budou obnovena v případě selhání systému nebo transakce.

OUTBUFF
Uvádí celkovou velikost úložiště, které má být použito IBM MQ pro výstupní vyrovnávací paměti pro zápis aktivních a archivních souborů dat protokolu, v kilobajtech. Každá výstupní vyrovnávací paměť má velikost 4 kB.

Parametr musí být v rozsahu od 128 do 4000. Uvedená hodnota je zaokrouhlena nahoru na násobek 4. Hodnoty mezi 40 a 128 budou akceptovány z důvodu kompatibility a jsou považovány za hodnotu 128.

Výchozí hodnota je 4000 KB.

Doporučené nastavení:

Testovací systém	400 KB

Produkční systém	4 000 KB Nastavte tuto hodnotu na maximum, abyste se vyhnuli překročení vyrovnávací paměti výstupu protokolu.

TWOACTV
Uvádí jednoduché nebo duální aktivní protokolování.

Uveďte buď:

NO
Jednotlivý aktivní protokol

YES
Duální aktivní protokoly

Výchozí hodnota je ANO.

Další informace o použití jednoho a duálního protokolování naleznete v tématu Správa prostředků produktu IBM MQ.

TWOARCH
Určuje počet protokolů archivu, které produkt IBM MQ produkuje, když je aktivní protokol odložen.

Uveďte buď:

NO
Jednoduché archivní protokoly

YES
Duální archivní protokoly

Výchozí hodnota je ANO.

Doporučené nastavení:

Testovací systém	NO
Produkční systém	ANO (výchozí)

Další informace o použití jednoho a duálního protokolování naleznete v tématu Správa prostředků produktu IBM MQ.

TWOBSDS
Určuje počet zaváděcích datových sad.

Uveďte buď:

NO
Jediný BSDS

YES
Duální BSDS

Výchozí hodnota je ANO.

Další informace o použití jednoho a duálního protokolování naleznete v tématu Správa prostředků produktu IBM MQ.

WRTHRSH
Uvádí počet výstupních vyrovnávacích pamětí o velikosti 4 kB, které mají být vyplněny, než jsou zapsány do aktivních datových sad protokolu.

Čím větší je počet vyrovnávacích pamětí, tím méně často dochází k zápisu, a tím se zlepší výkon produktu IBM MQ. Vyrovnávací paměti mohou být zapsány před tímto číslem, pokud se vyskytnou významné události, jako např. bod potvrzení.

Uveďte počet vyrovnávacích pamětí v rozsahu od 1 do 256.

Výchozí hodnota je 20.

V 9.1.2 **ZHYWRITE**

Uvádí, zda jsou zápisy do aktivních protokolů prováděny s povolenou technologií zHyperWrite. Datové sady aktivních protokolů musí být na nosičích podporujících technologii zHyperWrite, aby mohla být technologie zHyperWrite povolena.

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 822
Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6SYSP.

“Použití CSQ6ARVP” na stránce 835
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 835. 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

Tabulka 61. Výchozí hodnoty parametrů CSQ6ARVP (pokračování)			
Parametr	**Popis**	**Výchozí hodnota**	**Příkaz SET**
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
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 “Vytvoření zaváděcího programu a datových sad protokolu” na stránce 818.
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 “Vytvoření zaváděcího programu a datových sad protokolu” na stránce 818 a “Definujte sady stránek” na stránce 819.

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 viz Plánování na z/OS.

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; podrobnosti viz *z/OS Referenční příručka MVS JCL* a *z/OS Uživatelská příručka MVS JCL* .

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 viz Plánování na z/OS.

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 822
Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6SYSP.

“Použití CSQ6LOGP” na stránce 831
Toto téma použijte jako referenci, jak určit volby protokolování pomocí CSQ6LOGP.

V 9.1.0 z/OS *Použití CSQ6USGP*
Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6USGP .

Použijte CSQ6USGP k řízení záznamu použití produktu.

Výchozí parametry pro CSQ6USGP jsou zobrazeny v Tabulka 62 na stránce 842. Potřebujete-li změnit některou z těchto hodnot, přečtěte si podrobné popisy parametrů.

Upozornění: Pomocí příkazu SET SYSTEM nelze změnit žádné z těchto parametrů.

Tabulka 62. Výchozí hodnoty parametrů CSQ6USGP

Parametr	Popis	Výchozí hodnota
QMGRPROD	Produkt, na který se má zaznamenat použití správce front	Prázdný
AMSPROD	Produkt, proti kterému se má zaznamenat použití produktu Advanced Message Security (AMS)	Prázdný

QMGRPROD
Určuje produkt, pro který má být zaznamenán použití správce front.

Zadejte jednu z následujících možností:

MQ
Použití správce front je zaznamenáno jako samostatný produkt IBM MQ for z/OS s ID produktu 5655-MQ9.

VUE
Použití 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
V 9.1.3 Pokud tento parametr není nastaven, adresní prostor AMS se nespustí a zpráva CSQY024I bude výstupem.

Určuje produkt, proti kterému se má zaznamenat použití produktu Advanced Message Security , pokud se použije.

Zadejte jednu z následujících možností:

AMS
Využití funkce AMS je zaznamenáno jako samostatný produkt Advanced Message Security for z/OS s ID produktu 5655-AM9.

ROZŠÍŘENÝ
Použití AMS je zaznamenáno jako část produktu IBM MQ Advanced for z/OS s ID produktu 5655-AV9.

ADVANCEDVUE
Použití AMS je zaznamenáno jako část produktu IBM MQ Advanced for z/OS Value Unit Edition s ID produktu 5655-AV1.

Další informace o záznamu použití produktu naleznete v tématu Vytváření sestav o informacích o produktu .

Související odkazy

“Použití CSQ6SYSP” na stránce 822
Toto téma použijte jako referenci pro nastavení systémových parametrů pomocí CSQ6SYSP.

“Použití CSQ6LOGP” na stránce 831
Toto téma použijte jako referenci, jak určit volby protokolování pomocí CSQ6LOGP.

z/OS *Přizpůsobte parametry inicializátoru kanálu*

Pomocí příkazu ALTER QMGR můžete upravit inicializátor kanálu tak, aby vyhovoval vašim požadavkům.

- *Podle potřeby opakujte tuto úlohu pro každého správce front produktu IBM MQ .*
- *Tuto úlohu musíte provést při migraci z předchozí verze.*

Řada atributů správce front řídí způsob, jakým jsou distribuované fronty spouštěny. Nastavte tyto atributy pomocí příkazu MQSC ALTER QMGR. Ukázka inicializační datové sady thlqual.SCSQPROC(CSQ4INYG) obsahuje některá nastavení, která lze přizpůsobit. Další informace viz ALTER QMGR.

Hodnoty těchto parametrů se zobrazí jako série zpráv pokaždé, když spustíte inicializátor kanálu.

Vztah mezi adaptéry, dispečery a maximálním počtem kanálů

Parametry příkazu ALTER QMGR CHIADAPS a CHIDISPS definují počet řídicích bloků úloh (TCB) používaných inicializačním programem kanálu. CHIADAPS (adaptér) TCB se používají k vytvoření volání rozhraní API produktu IBM MQ do správce front. CHIDISPS (dispečer) TCB se používají pro volání do komunikační sítě.

Parametr ALTER QMGR MAXCHL ovlivňuje distribuci kanálů v rámci dispečerů TCB.

CHIDISPS

Máte-li malý počet kanálů, použijte výchozí hodnotu.

Jedna úloha pro každý procesor optimalizuje výkon systému. Vzhledem k tomu, že úlohy dispečeru jsou náročné na procesor, je třeba zachovat co nejméně málo úloh, aby byla minimalizována doba potřebná k vyhledání a spuštění podprocesů.

CHIDISPS (20) je vhodný pro systémy s více než 100 kanály. Je nepravděpodobné, že by došlo k významnému znevýhodnění v případě CHIDISPS (20), je-li to více dispečerů TCB, než je nezbytné.

Pokud máte více než 1000 kanálů, můžete povolit jeden dispečer pro každých 50 aktuálních kanálů. Například, uveďte CHIDISPS (40), chcete-li zpracovat až 2000 aktivních kanálů.

Pokud používáte protokol TCP/IP, je maximální počet dispečerů použitých pro kanály TCP/IP 100, a to i v případě, že v systému CHIDISPS zadáte větší hodnotu.

CHIADAPS

Každé volání rozhraní API produktu IBM MQ pro správce front je nezávislé na jiných systémech a lze je provést na libovolném adaptéru TCB. Volání používající trvalé zprávy mohou trvat mnohem déle, než je tomu u dočasných zpráv kvůli I/O protokolu. Proto může zpracování kanálu iniciátoru velkého počtu trvalých zpráv v rámci mnoha kanálů vyžadovat více než výchozí 8 adaptérů TCB pro optimální výkon. Je tomu tak zvláště tehdy, je-li velikost batchsize malá, protože zpracování dávkového zpracování také vyžaduje vstup/výstup protokolu a kde se používají kanály tenkého klienta.

Doporučená hodnota pro produkční prostředí je CHIADAPS (30). Použití více, než je nepravděpodobné, může poskytnout jakýkoli významný přínos navíc a je nepravděpodobné, že by byla jakákoliv významná nevýhoda v případě CHIADAPS (30), pokud se jedná o více TCB, než je nezbytné.

MAXCHL

Každý kanál je přidružen ke konkrétnímu dispečeru TCB při spuštění kanálu a zůstává přidružen k této TCB, dokud se kanál nezastaví. Každý TCB může sdílet mnoho kanálů. Hodnota MAXCHL se používá k šíření kanálů v rámci dostupných dispečerů TCB. První (MIN ((MAXCHL/CHIDISPS) , 10)) kanály, které se mají spustit, jsou přidruženy k prvnímu dispečeru TCB a tak dále, dokud se nebudou používat všechny dispečery TCB.

Dopad tohoto počtu na malý počet kanálů a velký MAXCHL je, že kanály nejsou rovnoměrně rozmístěné mezi dispečery. Pokud jste například nastavili CHIDISPS (10) a ponechal MAXCHL při výchozí hodnotě 200, ale měl pouze 50 kanálů, pět dispečerů by bylo asociováno s 10 kanály každý a pět by bylo nepoužité. Navrhujeme nastavení MAXCHL na počet kanálů, které se skutečně používají, kde se jedná o malé pevné číslo.

Změníte-li tuto vlastnost správce front, musíte také zkontrolovat vlastnosti správce front ACTCHL, LU62CHLa TCPCHL, abyste se ujistili, že jsou hodnoty kompatibilní. Úplný popis těchto vlastností a jejich vztah viz Parametry správce front .

Nastavení prostředí produktu z/OS UNIX System Services pro iniciátory kanálu

Inicializátor kanálu (CHINIT) používá podprocesy OMVS. Před vytvořením nové CHINIT nebo změnou počtu dispečerů nebo SSLTASKS zkontrolujte konfigurační parametry OMVS.

Každá CHINIT používá podprocesy 3 + CHIDISP + SSLTASKS OMVS. Tyto příspěvky přispívají k celkovému počtu podprocesů OMVS použitých v oblasti LPAR a k počtu podprocesů použitých ID uživatele spuštěných úloh CHINIT.

Můžete použít produkt **D OMVS,L** a zkontrolovat aktuální využití, využití vysoké vody a omezení systému MAXPROCSYS (maximální počet procesů, které systém povoluje).

Pokud přidáváte nové CHINIT nebo zvyšujete hodnoty parametrů CHIDISPS nebo SSLTASKS, musíte vypočítat nárůst podprocesů a zkontrolovat dopad na hodnoty MAXPROCSYS. Pomocí příkazu **SETOMVS** můžete dynamicky změnit hodnotu MAXPROCSYS nebo aktualizovat hodnotu parametru parmXPRCxx nebo obě.

Parametr OMVS MAXPROCUSER je počet vláken OMVS jednoho uživatele OMVS, který je se stejným UID, který může mít. Podprocesy se započítávají do této hodnoty. Takže pokud máte 2 CHINITS se stejným ID uživatele spuštěné úlohy, s 10 dispečery a 3 SSLTASKS, každý pak bude 2 * (3 +10 + 3) = 32 vláken pro UID OMVS.

Výchozí parametr MAXPROCUSER můžete zobrazit zadáním příkazu **D OMVS,O** a pomocí příkazu **SETOMVS** můžete dynamicky změnit hodnotu MAXPROCUSER nebo aktualizovat hodnotu parametru parmXPRCxx nebo obojí.

Tuto hodnotu můžete přepsat na bázi pro uživatele pomocí příkazu RACF **ALTUSER userid OMVS(PROCUSERMAX(nnnn))** nebo podobného.

Chcete-li spustit inicializátor kanálu, zadejte následující příkaz:

```
START CHINIT
```

Chcete-li se ujistit, že byl inicializátor kanálu úspěšně spuštěn, zkontrolujte, zda v protokolu úlohy xxxxCHIN(ssidCHIN) není chyba ICH408I .

Související pojmy

“Nastavení adaptérů dávek, TSO a RRS” na stránce 845
Zpřístupněte adaptéry pro aplikace tím, že přidáte knihovny do příslušných zřetězení STEPLIB. Chcete-li obstarávat výpisy paměti SNAP vydané adaptérem, přidělte jméno CSQSNAP DDname. Zvažte použití CSQBDEFV ke zlepšení přenositelnosti vašich aplikačních programů.

Záznamy dat statistiky inicializátoru kanálu

z/OS *Nastavení adaptérů dávek, TSO a RRS*

Zpřístupněte adaptéry pro aplikace tím, že přidáte knihovny do příslušných zřetězení STEPLIB. Chcete-li obstarávat výpisy paměti SNAP vydané adaptérem, přidělte jméno CSQSNAP DDname. Zvažte použití CSQBDEFV ke zlepšení přenositelnosti vašich aplikačních programů.

- *Tuto úlohu opakujte pro každého správce front produktu IBM MQ podle potřeby.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Chcete-li zpřístupnit adaptéry pro dávkové a jiné aplikace pomocí dávkových připojení, přidejte do struktury STEPLIB pro vaši dávkovou aplikaci následující knihovny produktu IBM MQ :

- thlqual.SCSQANL *x*
- thlqual.SCSQAUTH

kde *x* je jazyková písmena pro váš národní jazyk. (Tuto akci nemusíte provádět, pokud jsou knihovny v LPA nebo seznamu odkazů.)

Pro aplikace TSO přidejte knihovny do zřetězení STEPLIB v přihlašovacím postupu TSO nebo pomocí příkazu TSO TSOLIB aktivujte tyto knihovny.

Pokud adaptér zjistí neočekávanou chybu IBM MQ , odešle výpis paměti z/OS SNAP na DDname CSQSNAP a vydá do aplikace kód příčiny `MQRC_UNEXPECTED_ERROR` .Pokud příkaz CSQSNAP DD není v aplikaci JCL nebo CSQSNAP není přidělen k datové sadě pod TSO, žádný výpis paměti nebude proveden. Pokud k tomu dojde, můžete zahrnout příkaz CSQSNAP DD do JCL aplikace nebo alokovat CSQSNAP k datové sadě pod TSO a znovu spustit aplikaci. Avšak protože některé problémy jsou občasné, doporučujeme vám zahrnout příkaz CSQSNAP do JCL aplikace nebo alokovat CSQSNAP k datové sadě v proceduře přihlášení TSO, abyste zachytili příčinu selhání v době, kdy k němu dojde.

Dodaný program CSQBDEFV zlepšuje přenositelnost vašich aplikačních programů. V CSQBDEFV můžete zadat název správce front nebo skupiny sdílení front, které mají být připojeny, než abyste ji určoval v rámci volání `MQCONN` nebo `MQCONNX` v aplikačním programu. Můžete vytvořit novou verzi CSQBDEFV pro každého správce front nebo skupinu sdílení front. Postupujte takto:

1. Okopírujte program IBM MQ assembler CSQBDEFV z thlqual.SCSQASMS do uživatelské knihovny.
2. Dodaný program obsahuje výchozí název subsystému CSQ1. Tento název můžete uchovat pro testování a verifikaci instalace. V případě produkčních subsystémů můžete změnit název NAME=CSQ1 na název subsystému se čtyřmi znaky nebo použít řetězec CSQ1.

   Pokud používáte skupiny sdílení front, můžete místo hodnoty CSQ1zadat název skupiny sdílení front. Pokud tak učiníte, program vydá žádost o připojení k aktivnímu správci front v rámci této skupiny.
3. Sestavte a propojte program za účelem získání zaváděcího modulu CSQBDEFV. Pro sestavení zahrňte knihovnu thlqual.SCSQMACS do zřetězení SYSLIB; použijte parametry linkování `RENT,AMODE=31,RMODE=ANY`. Tato hodnota je zobrazena v ukázkovém JCL v souboru thlqual.SCSQPROC(CSQ4DEFV). Poté zahrňte zaváděcí knihovnu do tabulky z/OS Batch nebo TSO STEPLIB před thlqual.SCSQAUTH.

Související pojmy

“Nastavení operací a ovládacích panelů” na stránce 845

Chcete-li nastavit operace a ovládací panely, musíte nejprve nastavit knihovny, které obsahují požadované panely, EXECs, zprávy a tabulky. Abyste to mohli udělat, musíte vzít v úvahu, která národní jazyková funkce se má používat pro panely. Po provedení této akce můžete volitelně aktualizovat hlavní nabídku ISPF pro operace IBM MQ a ovládací panely a měnit nastavení funkčních kláves.

z/OS *Nastavení operací a ovládacích panelů*

Chcete-li nastavit operace a ovládací panely, musíte nejprve nastavit knihovny, které obsahují požadované panely, EXECs, zprávy a tabulky. Abyste to mohli udělat, musíte vzít v úvahu, která národní jazyková funkce se má používat pro panely. Po provedení této akce můžete volitelně aktualizovat hlavní nabídku ISPF pro operace IBM MQ a ovládací panely a měnit nastavení funkčních kláves.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Nastavení knihoven

Chcete-li nastavit operace IBM MQ a ovládací panely, postupujte takto:

1. Ujistěte se, že všechny knihovny obsažené ve vašich zřetězení jsou buď ve stejném formátu (F, FB, V, VB) a mají stejnou velikost bloku nebo jsou v pořadí zmenšujících se velikostí bloku. Jinak byste mohli mít problémy při pokusu o použití těchto panelů.
2. Zahrňte knihovnu thlqual.SCSQEXEC do zřetězení SYSEXEC nebo SYSPROC nebo ji aktivujte pomocí příkazu TSO ALTLIB. Tato knihovna, která je během instalace přidělena s formátem 80 záznamů s pevnou velikostí bloku, obsahuje požadované EXECs.

   Je vhodnější umístit knihovnu do zřetězení SYSEXEC. Pokud jej však chcete vložit do SYSPROC, musí mít knihovna délku záznamu 80 bajtů.
3. Přidejte thlqual.SCSQAUTH a thlqual.SCSQANLx do procedury přihlášení TSO STEPLIB nebo ji aktivujte pomocí příkazu TSO TSOLIB, pokud není uveden v seznamu odkazů nebo v LPA.
4. Můžete buď trvale přidat knihovny panelů IBM MQ do nastavení knihovny ISPF, nebo je povolit dynamicky nastavím při použití panelů. Pro předchozí volbu je třeba provést následující kroky:
   a. Zahrňte knihovnu obsahující operace a definice ovládacího panelu ve zřetězení ISPPLIB. Název je thlqual.SCSQPNLx, kde x je jazyková písmena pro váš národní jazyk.
   b. Zahrňte knihovnu obsahující požadované tabulky ve zřetězení ISPTLIB. Název je thlqual.SCSQTBLx, kde x je jazyková písmena pro váš národní jazyk.
   c. Zahrňte knihovnu obsahující požadované zprávy ve zřetězení ISPMLIB. Název je thlqual.SCSQMSGx, kde x je jazyková písmena pro váš národní jazyk.
   d. Zahrňte knihovnu obsahující požadované zaváděcí moduly do zřetězení ISPLLIB. Název této knihovny je thlqual.SCSQAUTH.
5. Otestujte, že máte přístup k panelům panelů IBM MQ z panelu příkazového procesoru TSO. Toto je obvykle volba 6 v menu primární volby ISPF/PDF. Název EXEC, který spustíte, je CSQOREXX.Nejsou žádné parametry, které byste měli uvést, pokud jste trvale umístili knihovny produktu IBM MQ do vašeho nastavení ISPF jako v kroku 4. Pokud jste nepoužili, použijte následující:

   ```
   CSQOREXX thlqual langletter
   ```

   kde `langletter` je písmeno označující národní jazyk, který má být použit:

   C
   Zjednodušená čínština

   E
   U.S. angličtina (smíšená velikost písmen)

   F
   Francouzština

   K
   japonština

   U
   U.S. Angličtina (velká písmena)

Aktualizace nabídky ISPF

Hlavní nabídku ISPF můžete aktualizovat, chcete-li povolit přístup k operacím produktu IBM MQ a k ovládacím panelům z ISPF. Požadované nastavení pro & ZSEL je:

```
CMD(%CSQOREXX thlqual langletter)
```

Informace o `thlqual` a `langletter`naleznete v kroku “5” na stránce 846.

Další podrobnosti naleznete v příručce *z/OS: ISPF Dialog Developer's Guide and Reference* .

Aktualizace funkčních kláves a nastavení příkazů

Běžné procedury ISPF můžete použít ke změně funkčních kláves a nastavení příkazů používaných panely. Identifikátor aplikace je CSQO.

To se však nedoporučuje, protože informace nápovědy nejsou aktualizovány tak, aby odrážely všechny provedené změny.

Související pojmy

“Zahrnout člena formátování výpisu paměti IBM MQ” na stránce 847
Chcete-li mít možnost formátovat výpisy paměti IBM MQ pomocí Interaktivního systému řízení problémů (IPCS), musíte aktualizovat některé systémové knihovny.

z/OS *Zahrnout člena formátování výpisu paměti IBM MQ*

Chcete-li mít možnost formátovat výpisy paměti IBM MQ pomocí Interaktivního systému řízení problémů (IPCS), musíte aktualizovat některé systémové knihovny.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Při migraci z předchozí verze je třeba provést tuto úlohu.*

Chcete-li mít možnost formátovat výpisy paměti IBM MQ pomocí systému IPCS (Interactive Problem Control System), zkopírujte datovou sadu thlqual.SCSQPROC(CSQ7IPCS) do SYS1.PARMLIB. Tuto datovou sadu byste neměli upravovat.

Pokud jste přizpůsobili proceduru TSO pro IPCS, thlqual.SCSQPROC(CSQ7IPCS) lze zkopírovat do libovolné knihovny v definici IPCSPARM. Podrobnosti o IPCSPARM naleznete v příručce *z/OS MVS IPCS Customization* .

Do zřetězení ISPPLIB musíte také zahrnout knihovnu thlqual.SCSQPNLA .

Chcete-li vytvořit programy pro formátování výpisu paměti dostupné pro vaši relaci TSO nebo IPCS, musíte do zřetězení STEPLIB zahrnout také knihovnu thlqual.SCSQAUTH nebo ji aktivovat pomocí příkazu TSO TSOLIB (i v případě, že již je v seznamu odkazů nebo v LPA).

Související pojmy

“Potlačit informační zprávy” na stránce 847
Systém IBM MQ může produkovat velké množství informačních zpráv. Můžete zabránit odeslání vybraných zpráv na konzolu nebo do protokolu pevné kopie.

z/OS *Potlačit informační zprávy*

Systém IBM MQ může produkovat velké množství informačních zpráv. Můžete zabránit odeslání vybraných zpráv na konzolu nebo do protokolu pevné kopie.

- *Tuto úlohu je třeba provést jednou pro každý systém z/OS , na kterém chcete spustit produkt IBM MQ.*
- *Při migraci z předchozí verze není třeba provést tuto úlohu.*

Je-li systém IBM MQ intenzivně využíván, je při zastavování a spouštění mnoha kanálů odesláno velké množství informačních zpráv do konzoly z/OS a do protokolu hardcopy. Most produktu IBM MQ - IMS a správce vyrovnávacích pamětí mohou také produkovat velké množství informačních zpráv.

V případě potřeby můžete některé z těchto zpráv konzoly potlačit použitím seznamu zařízení pro zpracování zpráv produktu z/OS určeného členy MPFLSTxx produktu SYS1.PARMLIB. Zprávy, které uvedete, se stále objeví v protokolu hardcopy, ale ne na konzole.

Ukázka thlqual.SCSQPROC(CSQ4MPFL) uvádí navrhované nastavení pro MPFLSTxx. Další informace o parametru MPFLSTxx najdete v příručce *z/OS MVS Initialization and Tuning Reference* .

Chcete-li potlačit vybrané informační zprávy v protokolu hardcopy, můžete použít instalační uživatelskou proceduru produktu z/OS IEAVMXIT. Pro požadované zprávy můžete nastavit následující bitové přepínače:

CTXTRDTM
Odstraňte zprávu.

Zpráva se nezobrazuje na konzolích nebo není protokolována v tištěné podobě.

CTXTESJL
Potlačit z protokolu úlohy.

Zpráva nevstupuje do protokolu úlohy JES.

CTXTNWTP.
Neprovádět zpracování WTP.

Zpráva se neodešle na terminál TSO ani na datovou sadu systémové zprávy dávkové úlohy.

Poznámka:

1. Podrobné informace o ostatních parametrech najdete v dokumentaci k produktu MVS Installation Exit .
2. Nedoporučuje se potlačit zprávy jiné než v navrženém seznamu potlačení, CSQ4MPFL.

Kromě toho můžete zadat další parametr:

EXCLMSG
Uvádí seznam zpráv, které mají být vyloučeny z jakéhokoli protokolu.

Zprávy v tomto seznamu se neodešlou do konzoly z/OS a do protokolu hardcopy. Další informace naleznete v části EXCLMSG v příručce “Použití CSQ6SYSP” na stránce 822 .

Související úlohy
“Testování správce front v systému z/OS” na stránce 863
Pokud jste správce front přizpůsobili nebo provedli migraci, 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 krok za krokem konfigurace skupiny sdílení front.

Pokud jste dokončili kroky v této části procesu pro nastavení vašeho systému IBM MQ for z/OS , měli byste “Přizpůsobte modul systémových parametrů.” na stránce 820 přidat data skupiny sdílení front. Chcete-li určit parametr QSGDATA, musíte upravit CSQ6SYSP .

z/OS *Nastavení prostředí produktu Db2*

Používáte-li skupiny sdílení front, musíte vytvořit požadované objekty produktu Db2 přizpůsobením a spuštěním počtu ukázkových úloh.

Nastavení prostředí produktu Db2

Musíte vytvořit a svázat požadované objekty produktu Db2 tím, že upravíte a spustíte několik ukázkových úloh.

- Zopakujte tuto úlohu pro každou skupinu sdílení dat produktu Db2 .
- Je třeba provést kroky `bind` a `grant` při migraci z předchozí verze.
- Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.

Budete-li později chtít používat skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Produkt IBM MQ poskytuje dvě ekvivalentní sady úloh. Ty s předponou CSQ45 jsou z důvodu kompatibility se staršími verzemi produktu IBM MQ a pro použití s produktem Db2 verze 11 a starší. Pokud nastavujete novou skupinu sdílení dat s Db2 V12 nebo novější, doporučujeme používat úlohy s předponou CSQ4X , protože tyto úlohy využívají nejnovější funkce Db2 pro dynamické velikosti a univerzální tabulkové prostory (UTS).

You must establish an environment in which IBM MQ can access and execute the Db2 plans that are used for queue sharing groups.

Pro každou novou skupinu sdílení dat produktu Db2 je třeba provést následující kroky. Všechny ukázky JCL se nacházejí v souboru thlqual.SCSQPROC.

1. Upravte a proveďte ukázku JCL CSQ45CSG V 9.1.0 (nebo CSQ4XCSG) , chcete-li vytvořit skupinu úložišť, která má být použita pro databázi IBM MQ , tabulkové prostory a tabulky.
2. Upravte a proveďte ukázku JCL CSQ45CDB V 9.1.0 (nebo CSQ4XCDB) k vytvoření databáze, kterou mají používat všichni správci front, kteří se připojují k této skupině sdílení dat produktu Db2 .
3. Upravte a proveďte ukázku JCL CSQ45CTS V 9.1.0 (nebo CSQ4XCTS) a vytvořte tabulkové prostory, které obsahují správce front a tabulky inicializátoru kanálu použité pro skupiny sdílení front (které mají být vytvořeny v kroku 1).
4. Upravte a proveďte ukázku JCL CSQ45CTB V 9.1.0 (nebo CSQ4XCTB) , abyste vytvořili 12 tabulek Db2 a přidružených indexů. Neměňte žádné názvy řádků nebo atributy.
5. Upravte a proveďte ukázku JCL CSQ45BPL , chcete-li svázat plány produktu Db2 pro správce front, obslužné programy a inicializátor kanálu.
6. Upravte a proveďte ukázku JCL CSQ45GEX , abyste udělili prováděcí oprávnění k plánům pro ID uživatelů, která jsou použita správcem front, obslužnými programy a inicializačním programem kanálu. ID uživatelů pro správce front a inicializátor kanálu jsou uživatelská jména, pod kterými jsou spuštěny procedury spuštěné úlohy. ID uživatele pro obslužné programy jsou ID uživatelů, pod kterými mohou být zadávaná dávková úloha zadána.

   Názvy příslušných plánů jsou zobrazeny v následující tabulce pro:

   - LTS Long Term Support verze ve sloupci LTS .
   - CD Continuous Delivery verze ve sloupci CD , kde n představuje vydání CD .

     V každém vydání n se zvyšuje o jedničku. Například v IBM MQ 9.0.3je CSQ5A90n CSQ5A903.

Uživatel	**Plány (LTS)**	**Plány (CD)**
Správce front	CSQ5A 910, CSQ5C 910, CSQ5D 910, CSQ5K 910, CSQ5L 910, CSQ5M 910, CSQ5P 910, CSQ5R 910, CSQ5S 910, CSQ5T 910, CSQ5U 910, CSQ5W 910	CSQ5A 91n, CSQ5C 91n, CSQ5D 91n, CSQ5K 91n, CSQ5L 91n, CSQ5M 91n, CSQ5P 91n, CSQ5R 91n, CSQ5S 91n, CSQ5T 91n, CSQ5U 91n, CSQ5W 91n
Funkce SDEFS obslužného programu dávky CSQUTIL	CSQ52 910	CSQ52 91n

Uživatel	Plány (LTS)	Plány (CD)
Obslužné programy CSQ5PQSG a CSQJUCNV	CSQ5B 910	CSQ5B 91n
Obslužný program služby CSQUZAP	CSQ5Z 910	CSQ5Z 91n

V případě selhání během instalace produktu Db2 je možné upravit a provést následující úlohy:

- CSQ45DTB pro zrušení tabulek a indexů.
- CSQ45DTS V 9.1.0 (nebo CSQ4XDTS) , chcete-li zrušit tabulkové prostory.
- CSQ45DDB V 9.1.0 (nebo CSQ4XDDB) pro zrušení databáze.
- CSQ45DSG V 9.1.0 (nebo CSQ4XDSG) , chcete-li zrušit skupinu úložišť.

Poznámka: Pokud tyto úlohy selžou kvůli problému s uzamčením Db2 , je to pravděpodobně způsobeno soupeřením o prostředek Db2 , zvláště je-li systém intenzivně využíván. Znovu odešlete úlohy později. Je vhodnější spouštět tyto úlohy, je-li systém lehce použit nebo uveden do klidového stavu.

Další informace o nastavení produktu Db2najdete v tématu Db2 Administration v příručce *Db2 for z/OS 11.0.0* .

Další informace o nastavení Db2najdete v tématu Db2 Administration v příručce *Db2 for z/OS 12.0.0* .

Informace o velikostech tabulek Db2 naleznete v příručce Plánování na z/OS .

Související pojmy

“Nastavení prostředku CF” na stránce 850

Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front v rámci skupiny sdílení front (QSG) v datové sadě zásad správy prostředků prostředku CF (CFRM) pomocí adaptéru IXCMIAPU.

z/OS *Nastavení prostředku CF*

Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front v rámci skupiny sdílení front (QSG) v datové sadě zásad správy prostředků prostředku CF (CFRM) pomocí adaptéru IXCMIAPU.

- Zopakujte tuto úlohu pro každou skupinu sdílení front.
- Možná budete muset provést tuto úlohu při migraci z předchozí verze.
- Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.

  Budete-li později chtít používat skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Všechny struktury pro skupinu sdílení front začínají s názvem skupiny sdílení front. Definujte následující struktury:

- Administrativní struktura s názvem *qsg-name* CSQ_ADMIN. Tato struktura je použita samostatně IBM MQ a neobsahuje žádná uživatelská data.
- Struktura systémové aplikace s názvem *qsg-name* CSQSYSAPPL. Tato struktura je používána systémovými frontami produktu IBM MQ k ukládání informací o stavu.
- Jedna nebo více struktur používaných k zadržení zpráv pro sdílené fronty. Ty mohou mít libovolný název, který vyberete až 16 znaků.
  - První čtyři znaky musí být název skupiny sdílení front. (Je-li název skupiny sdílení front kratší než čtyři znaky, musí být doplněn na čtyři znaky s symboly @.)
  - Pátý znak musí být abecední a následné znaky mohou být abecední nebo numerické. Tato část názvu (bez názvu skupiny sdílení front) je určena pro název CFSTRUCT, když definujete sdílenou frontu nebo objekt struktury CF.

V názvech struktur používaných k ukládání zpráv pro sdílené fronty můžete použít pouze abecední a číselné znaky, nemůžete použít žádné jiné znaky (například znak _, který se používá v názvu administrativní struktury).

Vzorové řídicí příkazy pro IXCMIAPU jsou v datové sadě thlqual.SCSQPROC(CSQ4CFRM). Upravte je a přidejte je do úlohy IXCMIAPU pro prostředek Coupling Facility a spusťte jej.

Když jste úspěšně definovali své struktury, aktivujte zásadu CFRM, která se používá. Chcete-li to provést, zadejte následující příkaz z/OS :

```
SETXCF START,POLICY,TYPE=CFRM,POLNAME= policy-name
```

Informace o strukturách prostředků CF a jejich velikostech naleznete v tématu Definování prostředků prostředku Coupling Facility.

Související pojmy

“Provádět ovládací prvky zabezpečení ESM” na stránce 814
Implementujte obslužné prvky zabezpečení pro správce front a inicializátor kanálu.

z/OS *Nastavit prostředí SMDS*

Chcete-li použít SMDS k odlehčování zpráv ve sdílených frontách, nastavte prostředí úložiště SMDS odlehčování.

- *Proveďte tuto úlohu pro každého správce front a strukturu ve skupině sdílení front, kterou chcete konfigurovat, chcete-li přesunout data do SMDS.*
- *Chcete-li konfigurovat další struktury pro předání dat do SMDS později, lze tuto úlohu provést znovu v daném čase.*
- *Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.*

  Chcete-li později použít skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Nastavit prostředí SMDS

1. Odhadněte strukturu a požadavky na prostor datové sady. Viz téma Pokyny týkající se kapacity sdílené datové sady zpráv.
2. Přidělit a předformátovat datové sady. Viz téma Vytvoření datové sady sdílených zpráv.
3. Při definování struktury prostředku CF pro produkt IBM MQse ujistěte, že jste definovali CFSTRUCT s CFLEVEL (5) a OFFLOAD (SMDS).

Související pojmy

“Nastavení prostředku CF” na stránce 850
Používáte-li skupiny sdílení front, definujte struktury prostředku Coupling Facility používané správci front v rámci skupiny sdílení front (QSG) v datové sadě zásad správy prostředků prostředku CF (CFRM) pomocí adaptéru IXCMIAPU.

z/OS *Přidejte položky IBM MQ do tabulek Db2 .*

Používáte-li skupiny sdílení front, spusťte obslužný program CSQ5PQSG pro přidání skupin sdílení front a položek správce front do tabulek IBM MQ ve skupině sdílení dat produktu Db2 .

- *Zopakujte tuto úlohu pro každou skupinu sdílení front produktu IBM MQ a každého správce front.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*
- *Tuto úlohu vynechte, pokud nepoužíváte skupiny sdílení front.*

  Chcete-li později použít skupiny sdílení front, proveďte tuto úlohu v daném okamžiku.

Pro každou skupinu sdílení front a každého správce front, který má být členem skupiny sdílení front, spusťte program CSQ5PQSG . (CSQ5PQSG je popsáno v publikaci Administrace IBM MQ for z/OS.)

Proveďte následující akce v uvedeném pořadí:

1. Přidejte položku skupiny sdílení front do tabulek produktu IBM MQ Db2 pomocí funkce ADD QSG programu CSQ5PQSG . Ukázku lze poskytnout v souboru thlqual.SCSQPROC(CSQ45AQS).

   Tuto funkci proveďte jednou pro každou skupinu sdílení front, která je definována ve skupině sdílení dat produktu Db2 . Před přidáním všech položek správce front, které odkazují na skupinu sdílení front, musí existovat položka skupiny sdílení front.
2. Přidejte položku správce front do tabulek produktu IBM MQ verze Db2 pomocí funkce ADD QMGR programu CSQ5PQSG . Ukázku lze poskytnout v souboru thlqual.SCSQPROC(CSQ45AQM).

   Tuto funkci 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. Chcete-li používat skupiny sdílení front, musí být spuštěna služba RRS.

Související pojmy

“Přizpůsobte modul systémových parametrů.” na stránce 820
Modul parametrů systému IBM MQ řídí prostředí protokolování, archivace, trasování a připojení, které IBM MQ používá při své operaci. Je dodán výchozí modul. Měli byste vytvořit svůj vlastní modul parametrů systému, protože některé parametry, například názvy datových sad, jsou obvykle specifické pro organizační jednotku.

z/OS *Implementovat ovládací prvky zabezpečení ESM pro skupinu sdílení front*

Implementujte ovládací prvky zabezpečení pro všechny správce front ve skupině sdílení front, přístup k serveru Db2 a ke strukturám seznamu prostředků Coupling Facility.

- *Zopakujte tuto úlohu pro každého správce front produktu IBM MQ ve skupině sdílení front.*
- *Při migraci z předchozí verze může být zapotřebí provést tuto úlohu.*

Zajistěte, aby ID uživatele přidružená ke správci front, inicializátor kanálu a obslužné programy měly oprávnění k vytvoření připojení RRSAF ke každému subsystému Db2 , s nímž chcete navázat připojení. ID uživatelů pro správce front a inicializátor kanálu jsou uživatelská jména, pod kterými jsou spuštěny procedury spuštěné úlohy.

ID uživatele pro obslužné programy jsou ID uživatelů, pod kterými mohou být zadávaná dávková úloha zadána. Profil RACF, ke kterému ID uživatele vyžaduje přístup pro čtení (READ), je `Db2ssid.RRSAF` ve třídě prostředků DSNR

ID uživatelů přidružená ke každému správci front ve skupině sdílení front musí být udělena odpovídající úroveň přístupu ke strukturám seznamu prostředku Coupling Facility. Třída RACF je FACILITY.

Následující ID uživatelů vyžadují přístup ALTER:

- ID správce front na profil produktu `IXLSTR.structure-name` .
- ID uživatele, které spouští CSQ5PQSG

Související pojmy

“Provádět ovládací prvky zabezpečení ESM” na stránce 814
Implementujte obslužné prvky zabezpečení pro správce front a inicializátor kanálu.

z/OS Konfigurace produktu Advanced Message Security for z/OS

Tato témata použijte jako krok za krokem průvodce konfigurací produktu Advanced Message Security (AMS).

Než začnete

Než začnete konfigurovat produkt AMS, ujistěte se, že byly provedeny následující kroky konfigurace správce front:

1. V 9.1.3 Od IBM MQ 9.1.3 ignorujte tento krok.

   U verzí produktu IBM MQ for z/OS starších než IBM MQ 9.1.3autorizovala APF knihovnu thqual.SDRQAUTH, jak je popsáno v “Autorizace APF pro zaváděcí knihovny produktu IBM MQ” na stránce 802.
2. Přidejte modul CSQ0DRTM do LPA, jak je popsáno v tématu “Aktualizovat seznam odkazů z/OS a LPA” na stránce 803.
3. Přidejte záznam pro CSQ0DSRV do tabulky vlastností programu z/OS (PPT), jak je popsáno v “Aktualizace tabulky vlastností programu z/OS” na stránce 807.
4. Zahrnout člena CSQ4INSM do zřetězení CSQINP2 spuštěné úlohy správce front, jak je popsáno v tématu “Upravit vstupní datové sady inicializace” na stránce 815.
5. V 9.1.3 V případě verzí produktu IBM MQ for z/OS starších než IBM MQ 9.1.3zahrňte do zřetězení STEPLIB správce front knihovnu thqual.SDRQAUTH , jak je popsáno v tématu “Vytvoření procedur pro správce front produktu IBM MQ” na stránce 811.

   Od IBM MQ 9.1.3 můžete povolit AMS pomocí atributu AMSPROD. Další podrobnosti viz Záznam využití produktu s produkty IBM MQ for z/OS.

Jak pokračovat dále

Konfigurujte zásady pro fronty chráněné produktem AMS. Zásady zabezpečení jsou popsány v části Administrace zásad zabezpečení produktu Advanced Message Security.

V tématu Příklady konfigurací na systému z/OSjsou k dispozici příklady konfigurací produktu AMS .

z/OS *Vytvořit procedury pro Advanced Message Security*

Každý subsystém IBM MQ , který má být konfigurován pro použití Advanced Message Security (AMS), vyžaduje katalogovou proceduru pro spuštění adresního prostoru AMS . Můžete vytvořit vlastní nebo použít knihovnu procedur dodané s produktem IBM.

Postup

1. Okopírujte ukázkovou proceduru spuštění úlohy *thlqual*.SCSQPROC (CSQ4AMSM) do vašeho SYS1.PROCLIB nebo, pokud nepoužíváte SYS1.PROCLIB, vaše knihovna procedur. Nazvěte proceduru xxxxAMSM, kde xxxx je název vašeho subsystému IBM MQ . Například CSQ1AMSM by byla procedura spuštění úlohy AMS pro správce front CSQ1.
2. Vytvořte kopii pro každý subsystém IBM MQ , který budete používat.
3. Přizpůsobte si postupy podle pokynů uvedených v ukázkové proceduře CSQ4AMSM. Symbolické parametry v souboru JCL můžete také použít k povolení úpravy procedury při jeho spuštění.
4. Zkontrolujte a případně změňte parametry předávané úloze AMS pomocí souboru Language Environment ® _CEE_ENVFILE. Ukázka thlqual.SCSQPROC(CSQ40ENV) obsahuje seznam podporovaných parametrů.
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 853

z/OS *Nastavení ID uživatele spuštěné úlohy Advanced Message Security*

Úloha Advanced Message Security (AMS) vyžaduje ID uživatele, které mu umožňuje být označováno jako proces UNIX System Services (USS).

Informace o této úloze

Kromě toho uživatelé, kterým úloha pracuje, musí mít také odpovídající definici UNIX UID (ID uživatele) a GID (ID skupiny), takže tito uživatelé jsou známí jako uživatelé produktu UNIX System Services. Další

informace o definování identifikátorů UID a GID služeb produktu UNIX naleznete v příručce *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS: UNIX Plánování systémových služeb porovnává tradiční zabezpečení UNIX se zabezpečením z/OS . Primární rozdíl mezi tradičním zabezpečením produktu UNIX a zabezpečením produktu z/OS spočívá v tom, že služby jádra podporují dvě úrovně odpovídajících oprávnění: úroveň UNIX a úroveň z/OS UNIX .

V závislosti na zásadách zabezpečení instalace může být úloha Advanced Message Security spuštěna buď s oprávněním superuživatele (uid (0)), nebo se svou identitou RACF povolenou pro třídu FACILITY RACF BPX.DAEMON a BPX.SERVER , protože tato úloha musí být schopna převzít identitu RACF svých uživatelů.

Je-li použita druhá metoda, nebo jste již aktivovali BPX.DAEMON nebo BPX.SERVER , program úlohy Advanced Message Security (thlqual.SCSQAUTH(CSQ0DSRV)) musí být umístěn v knihovnách řízených programem RACF .

Prostudujte si téma *z/OS: UNIX System Services Planning* a ujistěte se, že rozumíte bezpečnostním rozdílům mezi tradičním zabezpečením produktu UNIX a zabezpečením z/OS UNIX . To vám umožní spravovat úlohu Advanced Message Security podle zásady zabezpečení vaší instalace pro implementaci a spuštění privilegovaných procesů služeb systému UNIX .

Pro referenční účely jsou publikace užitečné pro tento přezkum:

- *z/OS: UNIX Plánování systémových služeb*
- *z/OS: Security Server RACF Security Administrator's Guide*

Poznámka: Zvolte ID uživatele pro tuto úlohu opatrně, protože certifikáty příjemce produktu Advanced Message Security se načtou do svazku klíčů přidruženého k tomuto ID uživatele. Tato úvaha je diskutována v tématu Použití certifikátů v systému z/OS .

Zde uvedené kroky popisují, jak nastavit uživatele spuštěné úlohy produktu Advanced Message Security . Tyto kroky používají jako příklady příkazy RACF . Používáte-li jiného správce zabezpečení, měli byste použít ekvivalentní příkazy.

Poznámka: Příklady v této sekci předpokládají, že jste aktivovali zpracování příkazu generického profilu pro třídy RACF STARTED, FACILITY, SURROGAT a kontrolu generických profilů. Další informace o tom, jak produkt RACF zachází s generickými profily, najdete v publikaci *z/OS: Security Server RACF Command Language Reference*.

Postup

1. Definujte uživatele spuštěné úlohy produktu Advanced Message Security na RACF. Příklady v této sekci používají ID uživatele WMQAMSM.

   ```
   ADDUSER WMQAMSM NAME('AMS user') OMVS (UID(0)) DFLTGRP(group)
   ```

   Vyberte výchozí 'skupinu', která odpovídá vašim instalačním standardům.

   Poznámka: Pokud nechcete udělit oprávnění uživatele USS superuživatele (UID (0)), musíte povolit ID uživatele produktu Advanced Message Security pro objekt BPX.DAEMON a BPX.SERVER profily třídy zařízení:

   ```
   PERMIT BPX.DAEMON CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
   ```

   a program úlohy Advanced Message Security (*thlqual*.SCSQAUTH (CSQ0DSRV)) musí být umístěn v knihovně řízené programem RACF .

   Chcete-li nastavit kontrolovaný program knihovny SCSQAUTH, můžete použít následující příkaz:

   ```
   RALTER PROGRAM * ADDMEM('thlqual.SCSQAUTH'//NOPADCHK) -or-
   RALTER PROGRAM ** ADDMEM('thlqual.SCSQAUTH'//NOPADCHK)
   SETROPTS WHEN(PROGRAM) REFRESH
   ```

Musíte také povolit řízení programu pro národní jazykovou knihovnu (*thlqual*.SCSQANLx), kterou používá úloha Advanced Message Security .

2. Určete, zda je třída RACF STARTED aktivní. Pokud není, aktivujte třídu STARTED RACF STARTED:

```
SETROPTS CLASSACT(STARTED)
```

3. Definujte profil spuštěné třídy pro úlohy produktu Advanced Message Security zadáním ID uživatele, které jste vybrali nebo jste vytvořili v kroku 1:

```
RDEFINE STARTED qmgrAMSM.* STDATA(USER(WMQAMSM))
```

kde *qmgr* je předpona názvu spuštěné úlohy. Spuštěná úloha může mít například název CSQ1AMSM. V tomto případě byste nahradil *qmgr*AMSM.* pomocí CSQ1AMSM.*.

Spuštěné úlohy AMS musí být pojmenovány *qmgr*AMSM.

4. Chcete-li aktualizovat profily třídy RACLISTed RACLISTed STARTED, použijte příkaz **SETROPTS** RACF :

```
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.

Je-li třída SURROGAT RACF aktivní, definuje jediný generický profil, který umožňuje úloze Advanced Message Security převzít identitu libovolného uživatele. Tato kontrola je ignorována, pokud třída SURROGAT není aktivní. Potřebné profily SURROGAT jsou popsány v příručce *z/OS: UNIX System Services Planning*.

Chcete-li definovat profily ve třídě SURROGAT:

a) Třídu SURROGAT produktu RACF aktivujte pomocí příkazu RACF SETROPTS:

```
SETROPTS CLASSACT(SURROGAT)
```

b) Aktivace zpracování generických profilů pro třídu RACF SURROGAT:

```
SETROPTS GENERIC(SURROGAT)
```

c) Aktivace zpracování příkazu generického profilu pro třídu RACF SURROGAT:

```
SETROPTS GENCMD(SURROGAT)
```

d) Definujte generický profil ve třídě SURROGAT:

```
RDEFINE SURROGAT BPX.SRV.* UACC(NONE)
```

e) Povolte ID uživatele produktu Advanced Message Security do generického profilu třídy SURROGAT:

```
PERMIT BPX.SRV.* CLASS(SURROGAT) ID(WMQAMSM) ACCESS(READ)
```

Poznámka: Můžete definovat více specifických profilů, chcete-li omezit určité uživatele, které mají být zpracovány úlohou Advanced Message Security , jak je popsáno v tématu *z/OS: UNIX Plánování služeb systému*.

Například profil s názvem BPX.SRV.MQUSER1 určuje, zda úloha AMS může převzít identitu ID uživatele MQUSER1.

f) Povolte ID uživatele produktu Advanced Message Security k prostředku BPX.SERVER (pokud již není provedeno v části Vytvoření certifikátů a klíčových řetězců):

```
PERMIT BPX.SERVER CLASS(FACILITY) ID(WMQAMSM) ACCESS(READ)
```

g) Pomocí příkazu **SETROPTS** RACF obnovte profily spuštěné třídy RACLISTed in-storage RACLISTS:

```
SETROPTS RACLIST(SURROGAT) REFRESH
SETROPTS RACLIST(FACILITY) REFRESH
```

6. Úloha produktu Advanced Message Security používá funkce poskytované službami z/OS System SSL k otevření klíčových kruhů spravovaných zařízením SAF. Nástroj SAF (System Authorization Facility), který přistupuje k obsahu svazků 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 FACILITY RACF . ID uživatele produktu Advanced Message Security proto musí být povoleno pro profily pomocí těchto příkazů:

   a) Pokud jste tak dosud neučinili, definujte generický profil produktu RACF pro třídu FACILITY produktu RACF , která chrání příkaz RACDCERT a volatelnou službu IRRSDL00 :

   ```
   RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
   SETROPTS RACLIST(FACILITY) REFRESH
   ```

   b) Udělte oprávnění ke spouštěným ID uživatele úlohy do generického profilu RACF :

   ```
   PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID(WMQAMSM) ACC(READ)
   ```

   Případně můžete do třídy RDATALIB udělit přístup pro čtení ke svazku klíčů uživatele úlohy datové služby, jak je uvedeno níže:

   ```
   PERMIT WMQASMD.DRQ.AMS.KEYRING.LST CLASS(RDATALIB) ID(WMQAMSM) ACC(READ)
   ```

7. Konfigurovat zabezpečení prostředků:

   a) Uživatel úlohy se spuštěnou úlohou produktu Advanced Message Security vyžaduje oprávnění k připojení ke správci front jako aplikaci dávky.

   Pokud má správce front povoleno zabezpečení připojení, udělte mu oprávnění úlohy AMS pro připojení ke správci front tímto příkazem:

   ```
   PERMIT hlq.BATCH CLASS(MQCONN) ID(WMQAMSM) ACC(READ)
   ```

   kde *hlq* může být buď název skupiny sdílení fronty názvů správce front.

   Další informace naleznete v tématu Profily zabezpečení připojení pro dávkové připojení.

   b) Uživatel spuštěné úlohy Advanced Message Security vyžaduje oprávnění k procházení systému SYSTEM.PROTECTION.POLICY.QUEUE.

   Je-li ve správci front aktivní zabezpečení fronty, udělte mu oprávnění uživatele AMS 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 fronty názvů správce front.

   Pokud správce front používá smíšené profily případů, definujte místo toho profil ve třídě MXQUEUE.

   Chcete-li spravovat zásady zabezpečení produktu AMS pomocí obslužného programu CSQ0UTIL , potřebují administrátoři přístup k vkládání zpráv do systému SYSTEM.PROTECTION.POLICY.QUEUE. To se provádí udělením přístupu UPDATE k profilu chránící frontu.

Další informace naleznete v tématu Profily pro zabezpečení fronty.

Jak pokračovat dále

"Udělte oprávnění RACDCCERT administrátorovi zabezpečení pro produkt Advanced Message Security" na stránce 857

z/OS Udělte oprávnění RACDCCERT administrátorovi zabezpečení pro produkt Advanced Message Security

Administrátor zabezpečení produktu Advanced Message Security vyžaduje oprávnění k použití příkazu RACDCERT pro vytváření a správu digitálních certifikátů.

Procedura

- Identifikujte odpovídající ID uživatele pro tuto roli a udělte oprávnění pro použití příkazu RACDCERT. Příklad:

```
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID(admin) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

  kde `admin` je ID uživatele vašeho administrátora zabezpečení produktu Advanced Message Security .

Jak pokračovat dále

"Udělte uživatelům oprávnění k prostředkům pro produkt Advanced Message Security" na stránce 857

z/OS Udělte uživatelům oprávnění k prostředkům pro produkt Advanced Message Security

Uživatelé produktu Advanced Message Security vyžadují příslušná oprávnění k prostředkům.

Informace o této úloze

Uživatelé Advanced Message Security , kteří jsou uživatelé, kteří vkládají nebo dostávají 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 pro umístění do SYSTEM.PROTECTION.ERROR.QUEUE

Úloha Advanced Message Security dočasně přebírá identitu svých klientů; to znamená, že úloha se chová jako náhrada ID uživatele z/OS uživatelů produktu Advanced Message Security během zpracování zpráv produktu IBM MQ do front, které jsou chráněny produktem Advanced Message Security.

Má-li úloha převzít identitu z/OS uživatele, musí mít ID uživatele klienta z/OS definovaný segment OMVS, který je přidružen k jeho uživatelskému profilu.

Jako administrativní pomůka poskytuje produkt RACF možnost definovat výchozí segment OMVS, který může být přidružen k uživatelským a skupinovým profilům RACF . Tato předvolba se použije, pokud ID uživatele nebo profil skupiny produktu z/OS nemá explicitně definovaný segment OMVS. Pokud plánujete mít velký počet uživatelů používajících produkt Advanced Message Security, můžete se rozhodnout použít tuto výchozí hodnotu, místo abyste výslovně definovali segment OMVS pro každého uživatele.

Příručka *z/OS: Security Server RACF Security Administrator's Guide* obsahuje podrobný postup pro definování výchozích segmentů OMVS. Projděte si proceduru popsanou v této příručce a určete, zda je definice výchozích segmentů OMVS v profilech uživatele a skupiny produktu RACF vhodná pro vaši instalaci.

Postup

1. Udělte oprávnění READ oprávnění k IRR.DIGTCERT.LISTRING profil ve třídě FACILITY:
   - Chcete-li udělit oprávnění READ pro IRR.DIGTCERT.LISTRING profil ve třídě FACILITY pro všechny uživatele, zadejte tento příkaz:

     ```
     RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(READ)
     ```

   - Chcete-li udělit oprávnění READ pro IRR.DIGTCERT.LISTRING profil ve třídě FACILITY na bázi uživatele, zadejte tento příkaz:

     ```
     PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(userid) ACCESS(READ)
     ```

     kde ID uživatele je jméno uživatele Advanced Message Security .
   - Případně můžete použít třídu RDATALIB k udělení přístupu ke specifickým kruhům klíčů. Oprávnění RDATALIB mají přednost před hodnotou IRR.DIGTCERT.LISTRING oprávnění. Příklad:

     ```
     PERMIT user.DRQ.AMS.KEYRING.LST CLASS(RDATALIB) ID(user) ACC(READ)
     ```

2. Používáte-li certifikáty správy ICSF a soukromé klíče, vyžadují uživatelé produktu Advanced Message Security přístup k určitým profilům 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
CSFSERV	CSFPKE	READ
CSFSERV	CSFPKD	READ
CSFSERV	CSFDSV	READ
KLÍČE CSFKEYS	Návěští ICSF PKDS	READ

3. Aplikace, které provádějí operace ve frontách s definovanými zásadami produktu AMS , potřebují přístup pro vkládání zpráv do systému SYSTEM.PROTECTION.ERROR.QUEUE. Udělte přístup k frontě 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 správce front, a *userID* je ID uživatele aplikace.

Jak pokračovat dále

“Vytvořit svazky klíčů pro Advanced Message Security” na stránce 858

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 . Než budete moci použít produkt AMS, musíte vytvořit tyto svazky klíčů a certifikáty.

Informace o této úloze

Produkt Advanced Message Security přistupuje k certifikátům v následujících klíčových kruzích:

- Jeden svazek klíčů vlastněný uživatelem adresního prostoru AMS .

- Klíčové řetězce vlastněné jednotlivými uživateli, které odesílají nebo přijímají zprávy ve frontách s definovanými zásadami produktu AMS .

Tyto klíčové kroužky musí být pojmenovány `drq.ams.keyring`.

Další informace o klíčových kruzích a certifikátech používaných produktem AMSa příklad scénáře najdete v tématu Použití certifikátů v systému z/OS.

Chcete-li vytvořit svazky klíčů vyžadované produktem AMSa připojit certifikáty ke klíčům klíčů, postupujte podle následujících kroků. Před spuštěním AMSmusíte vytvořit svazek klíčů, jehož vlastníkem je uživatel adresního prostoru AMS . Můžete vytvořit ty klíče, které vlastní uživatelé, kteří posílají nebo přijímají zprávy kdykoli.

Postup

1. Zadejte následující příkaz pro vytvoření svazku klíčů, jehož vlastníkem je uživatel 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 vydáním příkazu v kroku 1 pro každé ID uživatele.
3. Připojte certifikát certifikační autority (CA) pro vydavatele certifikátů uživatele do svazku klíčů vlastněného 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 jmenovka certifikátu CA.

   Používáte-li jako svou CA RACF a potřebujete vytvořit certifikát certifikační autority, postupujte podle příkladu v tématu Definování certifikátu lokálního vydavatele certifikátů.
4. Pokud používáte zásady zabezpečení ochrany soukromí nebo důvěrnosti k šifrování zpráv ve frontách chráněných produktem AMS, připojte certifikáty příjemců zpráv do svazku klíčů vlastněného 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 jmenovka certifikátu uživatele.

   Atribut `USAGE(SITE)` zabraňuje tomu, aby soukromý klíč byl přístupný v souboru svazku klíčů.

   Pokud vytváříte své vlastní certifikáty pomocí produktu RACF, postupujte podle příkladu v části Vytvoření digitálního certifikátu pomocí soukromého klíče , abyste vytvořili certifikát.
5. Připojte se k certifikátům každého uživatele, který odesílá nebo přijímá zprávy chráněné produktem AMS do svazku klíčů vlastněného daným uživatelem. Certifikát musí být připojen jako výchozí certifikát v souboru 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 jmenovka certifikátu uživatele.

Jak pokračovat dále

“PovolitAdvanced Message Security” na stránce 859

z/OS *PovolitAdvanced Message Security*

Schopnost zásady zabezpečení pro správce front je řízena parametrem SPLCAP v modulu parametru systému.

Informace o této úloze

Chcete-li povolit produkt Advanced Message Security (AMS) pro jednoho správce front, postupujte podle následujících kroků.

Tato úloha vyžaduje změnu modulu parametrů systému. Další informace o vytváření a úpravě modulu parametrů systému naleznete v příručce “Přizpůsobte modul systémových parametrů.” na stránce 820 .

Postup

1. Nastavte **SPLCAP** na YES v CSQ6SYSP. Další informace o makru CSQ6SYSP naleznete v příručce “Použití CSQ6SYSP” na stránce 822 .
2. V 9.1.3
   Produkt **AMSPROD** nastavte buď na AMS, ADVANCED, nebo ADVANCEDVUE v závislosti na oprávnění k licenci. Další informace o makru CSQ6USGP viz using CSQ6USGP .
3. Znovu zkompilujte modul parametrů systému.
4. Restartujte správce front s aktualizovaným modulem parametrů systému. Adresní prostor AMS se spustí automaticky při spuštění správce front.

V 9.1.0 z/OS Konfigurace serveru mqweb

Tato témata použijte jako krok za krokem ke konfiguraci serveru mqweb.

Související úlohy

“Konfigurace produktů IBM MQ Console a REST API” na stránce 735

Server mqweb, který je hostitelem produktů IBM MQ Console a REST API , je dodáván spolu s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh, jako je například konfigurace zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny volby konfigurace, které jsou k dispozici.

V 9.1.0 z/OS *Vytvoření serveru mqweb*

Pokud jste nainstalovali webové komponenty IBM MQ for z/OS UNIX System Services a chcete použít MQ Consolenebo REST API, musíte vytvořit a upravit server mqweb.

Než začnete

Musíte vytvořit SYSTEM.REST.REPLY.QUEUE pro použití serveru Liberty . Proveďte to pomocí nejnovější ukázky **CSQ4INSG** v souboru “Upravit vstupní datové sady inicializace” na stránce 815.

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 musíte provést jednou pro každý systém z/OS , kde chcete spustit MQ Console nebo REST API.
- Pro každou spuštěnou verzi produktu IBM MQ potřebujete server mqweb.
- Při migraci z předchozí verze může být nutné aktualizovat nebo upravit konfiguraci serveru.

MQ Console a REST API vyžadují vytvoření jednoho serveru Liberty s názvem mqweb.

Všechny soubory konfigurace serveru a soubory protokolu jsou uloženy v uživatelském adresáři Liberty .

Upozornění: Viz RACF profily , kde jsou některé příklady RDEFINE, a v sekci Profily použité k řízení přístupu k IBM MQ prostředkům viz Profily pro seznamy názvů , kde naleznete informace o nastavení nezbytného zabezpečení na serveru.

Chcete-li vytvořit server mqweb, postupujte takto:

Postup

1. 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 bude obsahovat soubory protokolu i konfiguraci serveru, měli byste tento adresář vytvořit 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 installation z/OS UNIX i souborový systém adresáře uživatelů Liberty buď zohledňují prostředí sysplex, nebo jsou lokálně připojeny k systému, kde je spuštěn server mqweb.
2. V systémových službách UNIX se ujistěte, že váš aktuální adresář je `PathPrefix/web/bin`, zadáním následujícího příkazu:

   ```
   cd PathPrefix/web/bin
   ```

   `PathPrefix` je instalační cesta ke komponentám systémových služeb systému IBM MQ UNIX.
3. Vytvořte adresář uživatelů Liberty obsahující definici serveru template mqweb spuštěním skriptu **`crtmqweb`** . Chcete-li například vytvořit adresář uživatelů Liberty v adresáři `/var/mqm/mqweb`, zadejte příkaz:

   ```
   ./crtmqweb /var/mqm/mqweb
   ```

   Poznámka: Skript **`crtmqweb`** přijímá jeden volitelný parametr-název uživatelského adresáře Liberty .

   Pokud nezadáte název pro adresář uživatelů Liberty , použije se výchozí hodnota `/var/mqm/web/installation1` .
4. Změňte vlastnictví adresářů a souborů v uživatelském adresáři Liberty tak, aby náležel 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 mqweb server” na stránce 862

Související úlohy

“Konfigurace produktů IBM MQ Console a REST API” na stránce 735

Server mqweb, který je hostitelem produktů IBM MQ Console a REST API , je dodáván spolu s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh, jako je například konfigurace zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny volby konfigurace, které jsou k dispozici.

V 9.1.0 z/OS *Vytvoření procedury pro mqweb server*

Pokud jste nainstalovali webové komponenty produktu IBM MQ for z/OS Unix System Services a chcete použít produkt MQ Consolenebo produkt REST API, je třeba vytvořit katalogovou proceduru pro spuštění serveru mqweb. Parametr mqweb server je server Liberty , který je hostitelem produktů MQ Console a REST API.

- Tuto úlohu musíte provést jednou pro každý systém z/OS , na kterém chcete spustit MQ Console nebo REST API.
- Pro každou verzi produktu IBM MQ , která je spuštěna, potřebujete mqweb server. Příklad: spuštěná úloha s názvem MQWB0910 pro správce front v produktu IBM MQ 9.1.0 a spuštěnou úlohu s názvem MQWB0905 pro správce front na serveru IBM MQ 9.0.5.

  Pokud máte v systému z/OS pouze jednoho správce front, můžete spustit jednu úlohu spuštěnou s jedním serverem produktu Liberty a změnit knihovny, které používá při migraci správce front.
- Při migraci z předchozí verze může být nutné upravit katalogizovanou proceduru.

Chcete-li vytvořit katalogizovanou proceduru, proveďte následující postup:

1. Zkopírujte ukázkovou proceduru spuštění úlohy `thlqual.SCSQPROC(CSQ4WEBS)` do knihovny procedur.

   Pojmenujte proceduru podle standardů vašeho podniku.

   Příklad: `MQWB0910`udává, že se jedná o katalogovou proceduru pro server IBM MQ 9.1.0 mqweb.
2. Přizpůsobte si postup podle pokynů v rámci výběrového řízení CSQ4WEBS.

   Povšimněte si, že uživatelský adresář Liberty je adresář určený při spuštění skriptu **crtmqweb** pro vytvoření definice mqweb serveru.

   Podrobnosti viz “Vytvoření serveru mqweb” na stránce 860.

   Poznámka: Při úpravě člena se ujistěte, že jste zadali parametr **Caps off** , protože tento soubor má malá data.
3. Autorizujte proceduru pro spuštění pod vaším externím správcem zabezpečení.
4. Tento adresní prostor klasifikujte pomocí správce WLM (IBM Workload Manager).

   Parametr mqweb je aplikací produktu IBM MQ a uživatelé pracují s touto aplikací. Aplikace nemusí být ve službě WLM vysoká důležitost a může být vhodná třída služeb **STCUSER** .

Další kroky

Chcete-li dokončit konfiguraci serveru mqweb, postupujte podle kroků v části “Základní konfigurace pro server mqweb” na stránce 735 .

Související úlohy

“Konfigurace produktů IBM MQ Console a REST API” na stránce 735

Server mqweb, který je hostitelem produktů IBM MQ Console a REST API , je dodáván spolu s výchozí konfigurací. Chcete-li použít některou z těchto komponent, je třeba dokončit řadu konfiguračních úloh,

jako je například konfigurace zabezpečení, aby se uživatelé mohli přihlásit. Toto téma popisuje všechny volby konfigurace, které jsou k dispozici.

z/OS Testování správce front v systému z/OS

Pokud jste správce front přizpůsobili nebo provedli migraci, 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 přizpůsobení produktu IBM MQ for z/OSmůžete použít dodaný program pro ověření instalace CSQ4IVP1, abyste potvrdili, že je produkt IBM MQ for z/OS funkční.

Základní program pro ověření instalace CSQ4IVP1 testuje nesdílené fronty a ověřuje základní produkt IBM MQ bez použití ukázek C, COBOL nebo CICS .

Po spuštění ověření základní instalace můžete provést test pro sdílené fronty pomocí rozhraní CSQ4IVP1 s různými frontami a také otestovat, zda jsou správně nastaveny produkty Db2 a prostředek Coupling Facility. Chcete-li potvrdit, že distribuované ukládání do fronty je v provozu, můžete použít dodaný program pro ověření instalace, CSQ4IVPX,

CSQ4IVP1 je dodáván jako zaváděcí modul a poskytuje sadu procedurálních ukázkových aplikací jako zdrojové moduly, které demonstrují typická použití rozhraní MQI (Message Queue Interface). Tyto zdrojové moduly můžete použít k testování různých prostředí programovacích jazyků. Můžete kompilovat a upravit odkaz-upravit podle toho, která z dalších ukázek je pro vaši instalaci vhodná, s použitím dodaného ukázkového souboru JCL dodaného.

Procedura

- Informace o tom, jak testovat správce front v systému z/OS, najdete v následujících dílčích tématech:
  - “Spuštění programu pro ověření základní instalace” na stránce 863
  - “Testování skupin sdílení front” na stránce 867
  - “Testování distribuovaných front” na stránce 868
  - “Testování programů v jazycích C, C + +, COBOL, PL/I a CICS s IBM MQ for z/OS” na stránce 871

Související pojmy

IBM MQ for z/OS koncepce

Související úlohy

Plánování vašeho prostředí IBM MQ na systému z/OS

“Konfigurace správců front v systému z/OS” na stránce 795
Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Správa serveruIBM MQ for z/OS

z/OS Spuštění programu pro ověření základní instalace

Po instalaci a přizpůsobení produktu IBM MQmůžete použít dodaný program pro ověření instalace CSQ4IVP1, abyste potvrdili, že je produkt IBM MQ funkční.

Základní program pro ověření instalace je dávkovým kompilátorem IVP, který ověřuje základní soubor IBM MQ bez použití ukázek C, COBOL nebo CICS .

Modul IVP produktu Batch Assembler IVP je upraven nástrojem SMP/E a moduly načtení jsou dodávány v knihovně thlqual.SCSQLOAD.

Po dokončení kroku SMP/E APPLY a kroků přizpůsobení spusťte program IVP produktu Batch Assembler IVP.

Další podrobnosti naleznete v těchto oddílech:

- Přehled aplikace CSQ4IVP1
- Příprava na spuštění CSQ4IVP1
- Spuštění CSQ4IVP1
- Kontrola výsledků CSQ4IVP1

Přehled aplikace CSQ4IVP1

CSQ4IVP1 je dávková aplikace, která se připojuje k subsystému IBM MQ a provádí tyto základní funkce:

- Vydá volání IBM MQ
- Komunikuje s příkazovým serverem
- Ověřuje, zda je spuštění aktivní
- Generuje a odstraní dynamickou frontu
- Ověřuje zpracování ukončení platnosti zprávy.
- Ověřuje zpracování potvrzení zprávy

Příprava na spuštění CSQ4IVP1

Před spuštěním příkazu CSQ4IVP1:

1. Zkontrolujte, zda se položky IVP nacházejí ve zřetězení datové sady CSQINP2 ve spouštěcím programu správce front. Položky IVP se dodávají v členu thlqual.SCSQPROC(CSQ4IVPQ). Pokud tomu tak není, přidejte do své zřetězení CSQINP2 definice uvedené v souboru thlqual.SCSQPROC(CSQ4IVPQ). Je-li správce front momentálně spuštěn, je třeba jej restartovat, aby se tyto definice mohly projevit.
2. Ukázkový kód JCL CSQ4IVPR, který je vyžadován ke spuštění ověřovacího programu instalace, je v knihovně thlqual.SCSQPROC.

   Upravte soubor JCL CSQ4IVPR s kvalifikátorem vyšší úrovně pro knihovny produktu IBM MQ , národní jazyk, který chcete použít, čtyřznakový název správce front produktu IBM MQ a místo určení pro výstup úlohy.
3. Aktualizujte produkt RACF tak, aby byl produkt CSQ4IVP1 povolen pro přístup k jeho prostředkům, je-li zabezpečení produktu IBM MQ aktivní.

   Chcete-li spustit CSQ4IVP1 , je-li zabezpečení produktu IBM MQ povoleno, potřebujete ID uživatele produktu RACF s oprávněním pro přístup k objektům. Podrobné informace o definování prostředků pro produkt RACFnaleznete v tématu Nastavení zabezpečení v systému z/OS . ID uživatele, který spouští IVP, musí mít následující přístupové oprávnění:

Oprávnění	Profil	Třída
READ	ssid.DISPLAY.PROCESS	MQCMDS
UPDATE	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
UPDATE	ssid.SYSTEM.COMMAND.REPLY.MODEL	MQQUEUE
UPDATE	ssid.CSQ4IVP1.**	MQQUEUE
READ	ssid.BATCH	MQCONN

   Tyto požadavky předpokládají, že zabezpečení produktu IBM MQ je aktivní. Příkazy RACF pro aktivaci zabezpečení produktu IBM MQ jsou zobrazeny v Obrázek 100 na stránce 865. Tento příklad předpokládá, že název správce front je CSQ1 a že ID uživatele, který spouští 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 100. Příkazy RACF pro CSQ4IVP1

Spuštění CSQ4IVP1

Pokud jste tyto kroky provedli, spusťte správce front. Je-li správce front již spuštěn a vy jste změnili CSQINP2, musíte správce front zastavit a restartovat jej.

Proces IVP se spouští jako dávková úloha. Upravte zakázkový list tak, aby odpovídal požadavkům na odeslání vaší instalace.

Kontrola výsledků CSQ4IVP1

IVP se dělí do 10 etap; každá fáze musí být dokončena s kódem dokončení nula, než se spustí další fáze. IVP generuje sestavu, vypisuje:

- Název správce front, ke kterému je připojen.
- Jedna jednořádková zpráva zobrazující kód dokončení a kód příčiny vrácený z každé fáze.
- Informační zpráva jednosměrně tam, kde je to vhodné.

Ukázková sestava je k dispozici v produktu Obrázek 101 na stránce 867

z/OS Vysvětlení kódů dokončení a kódu příčiny najdete v tématu Zprávy, dokončení a kódy příčiny produktuIBM MQ for z/OS.

Některé fáze mají více než jedno volání IBM MQ a v případě selhání je vydána zpráva označující specifické volání IBM MQ , které selhalo. Také v některých fázích IVP předkládá vysvětlující a diagnostické informace do pole komentáře.

Úloha IVP požaduje výlučnou kontrolu určitých objektů správce front, a proto by měla být jedním vláknem přes systém. Počet případů, kdy může být IVP spuštěn pro správce front, však není omezen.

Mezi funkce prováděné jednotlivými fázemi patří:

Fáze 1
Připojte se ke správci front zadáním volání rozhraní API MQCONN .

Fáze 2
Určete název vstupní fronty systémových příkazů, kterou používá příkazový server k načtení zpráv vzniklých při zpracování požadavku. Tato fronta přijímá požadavky na zobrazení z fáze 5.

Chcete-li to provést, posloupnost volání je:

1. Chcete-li otevřít objekt správce front, zadejte volání MQOPEN s určením názvu správce front.
2. Vydejte volání MQINQ a zjistěte název vstupní fronty příkazového systému.
3. Vydejte volání MQINQ , abyste zjistili informace o různých přepínačích událostí správce front.
4. Zadejte volání MQCLOSE , abyste zavřeli objekt správce front.

Při úspěšném dokončení této fáze se v poli pro komentář zobrazí název vstupní fronty příkazu systému.

Fáze 3
Otevřete inicializační frontu pomocí volání **MQOPEN** .

Tato fronta je otevřena v této fázi v očekávání zprávy spouštěče, která je doručena jako výsledek příkazového serveru, který odpovídá na požadavek z fáze 5. Fronta musí být otevřena pro vstup tak, aby splňovala kritéria spouštěče.

Fáze 4
Vytvořte trvalou dynamickou frontu pomocí volby CSQ4IVP1.MODEL fronta jako model. Dynamická fronta má stejné atributy jako model, ze kterého byla vytvořena. To znamená, že když jsou odpovědi z požadavku na příkazový server ve fázi 5 zapsány do této fronty, do inicializační fronty otevřené ve fázi 3 se zapíše zpráva spouštěče.

Po úspěšném dokončení této fáze je název trvalé dynamické fronty označen v poli komentáře.

Fáze 5
Zadejte požadavek na příkaz MQPUT1 do fronty příkazů příkazového serveru.

Zpráva typu MQMT_REQUEST je zapsána do vstupní fronty systémových příkazů požadující zobrazení procesu CSQ4IVP1. Deskriptor zprávy pro zprávu určuje trvalou dynamickou frontu vytvořenou ve fázi 4 jako frontu pro odpověď pro odezvu příkazového serveru.

Fáze 6
Vydejte požadavek **MQGET** z inicializační fronty. V této fázi se na inicializační frontě otevřené ve fázi 3 vydá příkaz GET WAIT s intervalem 1 minuta. Očekává se, že vrácená zpráva bude zprávou spouštěče generovanou ve zprávách odezvy příkazového serveru, které jsou zapisovány do fronty pro odpověď.

Fáze 7
Odstraňte trvalou dynamickou frontu vytvořenou ve fázi 4. Vzhledem k tomu, že fronta stále obsahuje zprávy, je použita volba MQCO_PURGE_DELETE.

Fáze 8

1. Otevřete dynamickou frontu.
2. MQPUT zprávu s nastaveným intervalem vypršení platnosti.
3. Čekejte, až zpráva vyprší.
4. Pokuste se o příkaz MQGET s prošlou zprávou
5. Fronta MQCLOSE. Fronta.

Fáze 9

1. Otevřete dynamickou frontu.
2. MQPUT a message.
3. Vydejte MQCMIT k potvrzení aktuální jednotky práce.
4. Zpráva MQGET.
5. Chcete-li tuto zprávu vrátit zpět, zadejte příkaz MQBACK.
6. ZMQGET stejnou zprávu a ujistěte se, že počet vrácení je nastaven na 1.
7. Chcete-li zavřít frontu, zadejte příkaz MQCLOSE.

Fáze 10
Odpojte se od správce front pomocí produktu **MQDISC**.

Po spuštění produktu IVP můžete odstranit všechny objekty, které již nepotřebujete.

Pokud se IVP nespustí úspěšně, vyzkoušejte každý krok ručně, abyste zjistili, která funkce selhala.

```
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 101. Ukázková sestava z CSQ4IVP1

z/OS Testování skupin sdílení front

Základní program pro ověření instalace CSQ4IVP1 testuje nesdílené fronty.

CSQ4IVP1 lze použít bez ohledu na to, zda je správce front členem skupiny sdílení front nebo ne. Po spuštění základního rozhraní IVP můžete otestovat sdílené fronty pomocí programu pro ověření instalace CSQ4IVP1 s různými frontami. Tento test také slouží k tomu, aby byl správně nastaven produkt Db2 a prostředek CF.

Příprava na spuštění CSQ4IVP1 pro skupinu sdílení front

Před spuštěním příkazu CSQ4IVP1:

1. Přidejte strukturu prostředku Coupling Facility, kterou IVP používá k datové sadě zásad CFRM, jak je popsáno v tématu “Nastavení prostředku CF” na stránce 850. Dodané ukázky používají strukturu s názvem APPLICATION1, ale tuto strukturu můžete změnit, pokud chcete.
2. Zkontrolujte, zda se položky IVP nacházejí ve zřetězení datové sady CSQINP2 ve spouštěcím programu správce front. Položky IVP se dodávají v členu thlqual.SCSQPROC(CSQ4IVPG). Pokud nejsou, přidejte definice uvedené v souboru thlqual.SCSQPROC(CSQ4IVPG) do zřetězení CSQINP2 . Je-li správce front momentálně spuštěn, je třeba jej restartovat, aby se tyto definice mohly projevit.
3. V případě potřeby změňte název struktury prostředku Coupling Facility použitý v souboru thlqual.SCSQPROC(CSQ4IVPG).
4. Ukázkový kód JCL CSQ4IVPSpožadovaný ke spuštění ověřovacího programu instalace pro skupinu sdílení front je v knihovně thlqual.SCSQPROC.

   Upravte soubor JCL CSQ4IVPS s kvalifikátorem vyšší úrovně pro knihovny produktu IBM MQ , národní jazyk, který chcete použít, čtyřznakový název správce front produktu IBM MQ a místo určení pro výstup úlohy.
5. Aktualizujte produkt RACF tak, aby byl produkt CSQ4IVP1 povolen pro přístup k jeho prostředkům, je-li zabezpečení produktu IBM MQ aktivní.

   Chcete-li spustit CSQ4IVP1 , je-li zabezpečení produktu IBM MQ povoleno, potřebujete ID uživatele produktu RACF s oprávněním pro přístup k objektům. Podrobné informace o definování prostředků pro produkt RACFnaleznete v tématu Nastavení zabezpečení v systému z/OS . ID uživatele, který spouští IVP, musí mít kromě požadavku na spuštění základního IVP také následující přístupové oprávnění:

Oprávnění	Profil	Třída
UPDATE	ssid.CSQ4IVPG.**	MQQUEUE

Tyto požadavky předpokládají, že zabezpečení produktu IBM MQ je aktivní. Příkazy RACF pro aktivaci zabezpečení produktu IBM MQ jsou zobrazeny v Obrázek 102 na stránce 868. Tento příklad předpokládá, že název správce front je CSQ1 a že ID uživatele, který spouští ukázku CSQ4IVP1 , je TS101.

```
RDEFINE MQQUEUE CSQ1.CSQ4IVPG.**
PERMIT CSQ1.CSQ4IVPG.** CLASS(MQQUEUE) ID(TS101) ACCESS(UPDATE)
```

Obrázek 102. Příkazy RACF pro CSQ4IVP1 pro skupinu sdílení front

Spuštění CSQ4IVP1 pro skupinu sdílení front

Pokud jste tyto kroky provedli, spusťte správce front. Je-li správce front již spuštěn a vy jste změnili CSQINP2, musíte správce front zastavit a restartovat jej.

Proces IVP se spouští jako dávková úloha. Upravte zakázkový list tak, aby odpovídal požadavkům na odeslání vaší instalace.

Kontrola výsledků CSQ4IVP1 pro skupinu sdílení front

IVP pro skupiny sdílení front funguje stejným způsobem jako základní IVP, až na to, že fronty, které se vytvoří, se nazývají CSQIVPG. *xx*. Chcete-li zkontrolovat výsledky IVP pro skupiny sdílení front, postupujte podle pokynů v příručce “Kontrola výsledků CSQ4IVP1” na stránce 865 .

z/OS Testování distribuovaných front

Dodaný program pro ověření instalace CSQ4IVPXmůžete použít k potvrzení, že distribuované fronty jsou v provozu.

Přehled úloh CSQ4IVPX

CSQ4IVPX je dávková úloha, která spouští inicializátor kanálu a vydává příkaz IBM MQ DISPLAY CHINIT. Tím je ověřeno, že všechny hlavní aspekty distribuovaných front jsou funkční a zároveň se vyhýbá potřebě nastavení definic kanálů a sítí.

Příprava na spuštění CSQ4IVPX

Před spuštěním skriptu CSQ4IVPX:

1. Ukázkový kód JCL CSQ4IVPX, který se požaduje ke spuštění ověřovacího programu instalace, je v knihovně thlqual.SCSQPROC.

   Upravte soubor JCL CSQ4IVPX s kvalifikátorem vyšší úrovně pro knihovny produktu IBM MQ , národní jazyk, který chcete použít, název správce front se čtyřmi znaky a místo určení pro výstup úlohy.
2. Aktualizujte produkt RACF tak, aby byl produkt CSQ4IVPX povolen pro přístup k jeho prostředkům, je-li zabezpečení produktu IBM MQ aktivní. Chcete-li spustit CSQ4IVPX , je-li zabezpečení produktu IBM MQ povoleno, potřebujete ID uživatele produktu RACF s oprávněním pro přístup k objektům. Podrobné informace o definování prostředků pro produkt RACFnaleznete v tématu Nastavení zabezpečení v systému z/OS . ID uživatele, který spouští IVP, musí mít následující přístupové oprávnění:

Oprávnění	Profil	Třída
CONTROL	ssid.START.CHINIT a ssid.STOP.CHINIT	MQCMDS
UPDATE	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
UPDATE	ssid.SYSTEM.CSQUTIL.*	MQQUEUE

Oprávnění	Profil	Třída
READ	ssid.BATCH	MQCONN
READ	ssid.DISPLAY.CHINIT	MQCMDS

Tyto požadavky předpokládají, že je definován profil zabezpečení připojení ssid.CHIN (jak ukazuje Profily zabezpečení připojení pro iniciátor kanálu) a že je aktivní zabezpečení produktu IBM MQ . Příkazy RACF , které se mají provést, jsou zobrazeny v Obrázek 103 na stránce 870. Tento příklad předpokládá:

- Název správce front je CSQ1 .
- ID uživatele, který spouští ukázku CSQ4IVPX je TS101
- Adresní prostor inicializátoru kanálu je spuštěn pod ID uživatele CSQ1MSTR .

3. Aktualizujte produkt RACF tak, aby umožňoval adresní prostoru inicializátoru kanálu následující oprávnění k přístupu:

Oprávnění	Profil	Třída
READ	ssid.CHIN	MQCONN
UPDATE	ssid.SYSTEM.COMMAND.INPUT	MQQUEUE
UPDATE	ssid.SYSTEM.CHANNEL.INITQ	MQQUEUE
UPDATE	ssid.SYSTEM.CHANNEL.SYNCQ	MQQUEUE
ALTER	ssid.SYSTEM.CLUSTER.COMMAND.QUEUE	MQQUEUE
UPDATE	ssid.SYSTEM.CLUSTER.TRANSMIT.QUEUE	MQQUEUE
ALTER	ssid.SYSTEM.CLUSTER.REPOSITORY.QUEUE	MQQUEUE
CONTROL	ssid.CONTEXT.**	MQADMIN

Příkazy RACF se také zobrazí v Obrázek 103 na stránce 870.

```
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 103. Příkazy RACF pro CSQ4IVPX

Spuštění CSQ4IVPX

Pokud jste tyto kroky provedli, spusťte správce front.

Proces IVP se spouští jako dávková úloha. Upravte zakázkový list tak, aby odpovídal požadavkům na odeslání vaší instalace.

Kontrola výsledků CSQ4IVPX

CSQ4IVPX spustí obslužný program CSQUTIL IBM MQ , aby vydal tři příkazy MQSC. Datová sada výstupu SYSPRINT by měla vypadat jako Obrázek 104 na stránce 871, ačkoli podrobnosti se mohou lišit v závislosti na atributech správce front.

- Měli byste se podívat na příkazy **(1)** , za kterými následuje několik zpráv.
- Poslední zpráva z každého příkazu by měla být "CSQ9022I ... NORMÁLNÍ DOKONČENÍ" **(2)**.
- Úloha jako celek by měla být dokončena s návratovým kódem nula **(3)**.

```
CSQU000I CSQUTIL IBM MQ for z/OS - V6
CSQU001I CSQUTIL Queue Manager Utility - 2005-05-09 09:06:48
COMMAND
CSQU127I CSQUTIL Executing COMMAND using input from CSQUCMD data set
CSQU120I CSQUTIL Connecting to queue manager CSQ1
CSQU121I CSQUTIL Connected to queue manager CSQ1
CSQU055I CSQUTIL Target queue manager is CSQ1
START CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM138I +CSQ1 CSQMSCHI CHANNEL INITIATOR STARTING
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000000
CSQ9022I +CSQ1 CSQXCRPS ' START CHINIT' NORMAL COMPLETION
(2)
DISPLAY CHINIT
(1)
CSQN205I  COUNT=    2, RETURN=00000000, REASON=00000004
CSQM137I +CSQ1 CSQMDDQM DISPLAY CHINIT COMMAND ACCEPTED
CSQN205I  COUNT=   12, RETURN=00000000, REASON=00000000
CSQX830I +CSQ1 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 104. Příklad výstupu z CSQ4IVPX

z/OS Testování programů v jazycích C, C + +, COBOL, PL/I a CICS s IBM MQ for z/OS

Můžete testovat jazyky C, C + +, COBOL, PL/I nebo CICSpomocí ukázkových aplikací dodaných s produktem IBM MQ.

IVP (CSQ4IVP1) je dodáván jako zaváděcí modul a poskytuje ukázky jako zdrojové moduly. Tyto zdrojové moduly můžete použít k testování různých prostředí programovacích jazyků.

Další informace o ukázkových aplikacích najdete v tématu Ukázkové programy pro produkt IBM MQ for z/OS .

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 872.

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 796.
- 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 891.

Související pojmy

“nastaveníIBM MQ for z/OS” na stránce 800
Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ for z/OS .

Související úlohy

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče 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 se zpráva CSQM130I odešle vydavateli příkazu, který 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 “Provádět ovládací prvky zabezpečení ESM” na stránce 814.

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 800
Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ for z/OS .

Související úlohy

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

z/OS Definování objektů IBM MQ

Použijte jednu z metod vstupu příkazu IBM MQ k definování objektů IBM MQ . Další podrobnosti o definování těchto objektů naleznete v informacích v tomto tématu.

Informace o definování objektů naleznete v příručce “Monitorování a řízení kanálů v systému z/OS” na stránce 875 .

Přenosové fronty a spouštěcí kanály

Definujte následující:

- Lokální fronta s využitím XMITQ pro každý odesílající kanál zpráv.
- Definice vzdálených front.

  Objekt vzdálené fronty má tři různé použití, v závislosti na způsobu, jakým je zadán název a obsah:

  – Definice vzdálené fronty
  – Definice aliasu správce front
  – Definice alias fronty pro odpověď

  Tyto tři způsoby jsou zobrazeny v části Tři způsoby použití objektu definice vzdálené fronty.

Použijte pole TRIGDATA v přenosové frontě pro spuštění uvedeného kanálu. Příklad:

```
DEFINE QLOCAL(MYXMITQ) USAGE(XMITQ) TRIGGER +
INITQ(SYSTEM.CHANNEL.INITQ) TRIGDATA(MYCHANNEL)
DEFINE CHL(MYCHANNEL) CHLTYPE(SDR) TRPTYPE(TCP) +
XMITQ(MYXMITQ) CONNAME('9.20.9.30(1555)')
```

Dodaný vzorek CSQ4INYD uvádí další příklady nezbytných definic.

z/OS Ztráta konektivity ke struktuře prostředku mezipaměti klastru, kde je definována fronta synchronizace pro sdílené kanály nebo podobné problémy, může dočasně zabránit spuštění kanálu. Pokud při řešení problému používáte typ spouštěče FIRST a kanál se při spuštění nespustí, je třeba spustit kanál ručně. Chcete-li automaticky spustit spuštěné kanály po vyřešení problému, zvažte nastavení atributu TRIGINT správce front na jinou hodnotu než výchozí. Nastavení atributu TRIGINT na jinou hodnotu než výchozí nastavení způsobí, že inicializátor kanálu bude periodicky spouštět kanál, zatímco v přenosové frontě jsou zprávy.

Fronta synchronizace

DQM vyžaduje frontu pro použití s pořadovými čísly a identifikátory logických jednotek práce (LUWID). Musíte se ujistit, že je fronta k dispozici s názvem SYSTEM.CHANNEL.SYNCQ (viz Plánování na z/OS). Tato fronta musí být dostupná, jinak nelze spustit inicializátor kanálu.

Ujistěte se, že jste definovali tuto frontu pomocí INDXTYPE (MSGID). Tento atribut zlepšuje rychlost, ke které je možné přistupovat.

Fronty příkazů kanálu

Je třeba zajistit, aby pro systém existovala fronta příkazů kanálu s názvem SYSTEM.CHANNEL.INITQ.

Pokud inicializátor kanálu zjistí problém s parametrem SYSTEM.CHANNEL.INITQnebude moci normálně pokračovat, dokud nebude problém odstraněn. Problém může být jeden z následujících:

- Fronta je plná
- Fronta není povolena pro vložení
- Sada stránek, na které je fronta zapnuta, je plná.
- Inicializátor kanálu nemá správné oprávnění zabezpečení pro frontu.

Pokud se definice fronty změní na GET (DISABLED), zatímco inicializátor kanálu běží, iniciátor není schopen získat zprávy z fronty a ukončuje se.

Spuštění inicializátoru kanálu

Spouštěcí impuls je implementován pomocí inicializátoru kanálu. V systému IBM MQ for z/OSje iniciátor spuštěn s příkazem MQSC `START CHINIT`.

Zastavení inicializátoru kanálu

Inicializátor kanálu se zastaví automaticky při zastavení správce front. Potřebujete-li zastavit iniciátor kanálu, ale ne správce front, můžete použít příkaz MQSC `STOP CHINIT`.

z/OS Monitorování a řízení kanálů v systému z/OS

Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front.

Každý správce front produktu z/OS má program DQM (*inicializátor kanálu*). pro řízení propojení se vzdálenými správci front pomocí nativních zařízení produktu z/OS .

Implementace těchto panelů a příkazů v systému z/OS je integrována do operací a řídicích panelů a příkazů MQSC. V uspořádání těchto dvou sad panelů a příkazů se neodlišují žádné rozdíly.

Příkazy lze zadávat také pomocí příkazů PCF (Programmable Command Format). Informace o použití těchto příkazů najdete v tématu Automatizace administrativních úloh .

Informace v této sekci se používají ve všech případech, kdy se používá inicializátor kanálu pro distribuované řazení do fronty. Používá se k tomu, zda používáte skupiny sdílení front nebo řazení do front v rámci skupiny.

Řídicí funkce kanálu DQM

Přehled modelu správy distribuovaných front viz “Odeslání a příjem zprávy” na stránce 192.

Řídicí funkce kanálu se skládá z panelů, příkazů a programů, dvou synchronizačních front, front příkazů kanálů a definic kanálů. Toto téma je stručným popisem komponent funkce řízení kanálů.

- Definice kanálů jsou uchovávány jako objekty na stránce nastavené jako nula nebo v Db2, stejně jako další objekty IBM MQ v z/OS.
- Použijte operace a řídicí panely, příkazy MQSC nebo příkazy PCF pro:
  - Vytvořit, kopírovat, zobrazit, změnit a odstranit definice kanálu
  - Spustit a zastavit iniciátory kanálu a moduly listener
  - Kanály pro spuštění, zastavení a testování spojení, resetování pořadových čísel kanálů a řešení sporných zpráv, pokud nelze znovu zavést odkazy
  - Zobrazení informací o stavu kanálů
  - Zobrazit informace o aplikaci DQM

  Konkrétně můžete použít vstupní datovou sadu inicializace CSQINPX pro zadání příkazů MQSC. Tato sada může být zpracována pokaždé, když spustíte inicializátor kanálu. Další informace viz téma Inicializační příkazy.
- Existují dvě fronty (SYSTEM.CHANNEL.SYNCQ a SYSTEM.QSG.CHANNEL.SYNCQ) používaný pro účely opětného synchronizace kanálu. Definujte tyto fronty s INDEXTYPE (MSGID) z důvodu výkonu.
- Fronta příkazů kanálu (SYSTEM.CHANNEL.INITQ) se používá k ukládání příkazů pro iniciátory kanálu, kanály a moduly listener.
- Řídicí program kanálu pracuje ve svém vlastním adresním prostoru, odděleném od správce front a skládá se z iniciátoru kanálu, modulů listener, agentů MCA, monitoru spouštěčů a obslužné rutiny příkazů.

- Informace o skupinách sdílení front a sdílených kanálech naleznete v tématu Sdílené fronty a skupiny sdílení front.
- Pro řazení do front v rámci skupiny naleznete informace v tématu Řazení do front v rámci skupiny

Správa kanálů v systému z/OS

Pomocí odkazů v následující tabulce naleznete informace o správě kanálů, inicializátorů kanálů a modulů listener:

Tabulka 64. Úlohy kanálu

Úloha, která má být provedena	**Příkaz MQSC**
Definovat kanál	Definovat kanál
Změna definice kanálu	ALTER CHANNEL
Zobrazení definice kanálu	DISPLAY CHANNEL
Odstranit definici kanálu	Odstranit kanál
Spustit inicializátor kanálu	START CHINIT
Zastavit inicializátor kanálu	STOP CHINIT
Zobrazit informace o inicializátoru kanálu	DISPLAY CHINIT
Spuštění modulu listener kanálu	Spustit listener
Zastavení modulu listener kanálu	Ukončit listener
Spuštění kanálu	Spustit kanál
Testovat kanál	Odeslat signál Ping pro kanál
Resetovat pořadová čísla zpráv pro kanál	Resetovat kanál
Vyřešit neověřené zprávy na kanálu	Vyřešit kanál
Zastavení kanálu	Ukončit kanál
Zobrazení stavu kanálu	ZOBRAZIT STAV CHSTATUS
Zobrazit kanály klastru	ZOBRAZIT CLUSQMGR

Související pojmy

“Použití panelů a příkazů” na stránce 877
Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo operace a ovládací panely.

“nastaveníIBM MQ for z/OS” na stránce 800
Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ for z/OS .

“Nastavení komunikace pro z/OS” na stránce 891
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení určené v definici kanálu. Chcete-li uspět, je nutné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak definovat připojení.

“Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front” na stránce 896
Pomocí pokynů v této části můžete konfigurovat distribuované řazení do front se skupinami sdílení front v systému IBM MQ for z/OS.

“Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front” na stránce 900
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení zadané v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby připojení bylo definováno a k dispozici.

Související úlohy

“Konfigurace distribuovaných front” na stránce 171

Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 871
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 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 105 na stránce 877 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 105. 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 106 na stránce 878 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 106. Výpis kanálů

z/OS *Definování kanálu v systému z/OS*

V systému z/OSmůžete definovat kanál pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li definovat kanál pomocí příkazů MQSC, použijte DEFINE CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	2 (Definovat jako)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	
Dispozice	Umístění nového objektu.

Zobrazí se některé panely s informacemi o názvu a atributech, které chcete definovat pro kanál, který definujete. Inicializují se s výchozími hodnotami atributů. Před stisknutím klávesy Enter změňte všechny požadované hodnoty.

Poznámka: Pokud jste do pole **`object type`** zadali parametr CHANNEL, zobrazí se nejprve panel Vyberte platný typ kanálu.

Chcete-li definovat kanál se stejnými atributy jako existující kanál, zadejte název kanálu, který chcete zkopírovat, do pole **Name** na počátečním panelu. Panely jsou inicializovány s atributy existujícího objektu.

Další informace o atributech kanálů naleznete v tématu Atributy kanálu

Poznámka:

1. Pojmenujte všechny kanály v síti jedinečně. Jak je zobrazeno v Síťový diagram zobrazující všechny kanály, včetně názvů zdrojového a cílového správce front v názvu kanálu je dobrý způsob, jak toto pojmenování provést.

Poté, co jste definovali svůj kanál, je třeba kanál zabezpečit, viz “Zabezpečení kanálu” na stránce 880

z/OS *Změna definice kanálu*

Definici kanálu můžete změnit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li změnit definici kanálu pomocí příkazů MQSC, použijte příkaz ALTER CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	3 (Změnit)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.ALTER
Dispozice	Umístění uloženého objektu.

Zobrazí se některé panely obsahující informace o aktuálních atributech kanálu. Změňte všechna nechráněná pole, která mají být přepsáním nové hodnoty, a poté stiskněte klávesu Enter, abyste změnili definici kanálu.

Další informace o atributech kanálů naleznete v tématu Atributy kanálu.

z/OS *Zobrazení definice kanálu*

Definici kanálu můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit definici kanálu pomocí příkazů MQSC, použijte DISPLAY CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	1 (Seznam nebo zobrazení)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.DISPLAY
Dispozice	Umístění objektu.

Zobrazí se některé panely se zobrazením informací o aktuálních atributech kanálu.

Další informace o atributech kanálů naleznete v tématu Atributy kanálu.

z/OS *Odstranění definice kanálu*

Definici kanálu můžete odstranit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li odstranit definici kanálu pomocí příkazů MQSC, použijte příkaz DELETE CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	4 (Spravovat)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.DELETE

Pole	Hodnota
Dispozice	Umístění objektu.

Zobrazí se vám jiný panel. Na tomto panelu vyberte typ funkce 1.

Stisknutím klávesy Enter odstraníte definici kanálu; budete požádáni o potvrzení, že chcete definici kanálu odstranit opětovným stisknutím klávesy Enter.

Poznámka: Inicializátor kanálu musí být spuštěn před odstraněním definice kanálu (s výjimkou kanálů připojení klienta).

z/OS *Zobrazení informací o inicializátoru kanálu*

Informace o inicializátoru kanálu můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit informace o inicializátoru kanálu pomocí příkazů MQSC, použijte příkaz DISPLAY CHINIT.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	1 (Zobrazit)
Typ objektu	SYSTEM
Název	Prázdný

Zobrazí se vám jiný panel. Na tomto panelu vyberte typ funkce 1.

Poznámka:

1. Zobrazení distribuovaných informací o frontách může nějakou dobu trvat, pokud máte mnoho kanálů.
2. Inicializátor kanálu musí být spuštěn, než budete moci zobrazit informace o distribuovaných frontách.

z/OS *Zabezpečení kanálu*

Kanál můžete zabezpečit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zabezpečit kanál pomocí příkazů MQSC, použijte SET CHLAUTH.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	8

Zobrazí se editor, v němž můžete zadat příkaz MQSC, v tomto případě příkaz CHLAUTH, viz Obrázek 107 na stránce 880. Po dokončení zápisu do příkazu je třeba použít znaménko plus (+). Zadejte příkaz PF3 , chcete-li ukončit práci editoru a zadejte příkaz na příkazový server.

```
****************************** Top of Data ******************************
000001 SET CHLAUTH(SYSTEM.DEF.SVRCONN) +
000002 TYPE(SSLPEERMAP) +
000003 SSLPEER('CN="John Smith"') +
000004 MCAUSER('PUBLIC')
****** ***************************** Bottom of Data ****************************

Command ===>                          Scroll ===> PAGE
F1=Help   F3=Exit   F4=LineEdit F12=Cancel
```

Obrázek 107. Zadání příkazů

Výstup příkazu se poté zobrazí, viz Obrázek 108 na stránce 881

```
****** ***************************** 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 108. Výstup příkazu

z/OS *Spuštění inicializátoru kanálu*

Inicializátor kanálu můžete spustit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li spustit inicializátor kanálu s použitím příkazů MQSC, použijte příkaz START CHINIT.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	6 (Začátek)
Typ objektu	SYSTEM
Název	Prázdný

Zobrazí se panel Spuštění systémových funkcí. Text na následujícím panelu vysvětluje, jaká akce se má provést:

```
Start a System Function

Select function type, complete fields, then press Enter to start system
function.

Function type . . . . . _   1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
JCL substitution . . . . . ________________________________________________
________________________________________

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP
LU name (LU6.2) . . . . . ________________
Port number (TCP/IP) . . . 1414
IP address (TCP/IP) . . . ________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 109. Spuštění systémové funkce

Vyberte funkci typu 1 (inicializátor kanálu) a stiskněte klávesu Enter.

z/OS Zastavení inicializátoru kanálu

Inicializátor kanálu můžete zastavit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zastavit iniciátor kanálu pomocí příkazů MQSC, použijte příkaz STOP CHINIT.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	7 (Zastavit)
Typ objektu	SYSTEM
Název	Prázdný

Zobrazí se panel Zastavení systémových funkcí. Text následující po panelu vysvětluje, jak použít tento panel:

```
Stop a System Function

Select function type, complete fields, then press Enter to stop system
function.

Function type . . . . . _   1. Channel initiator
2. Channel listener
Action queue manager . . . : MQ25

Channel initiator
Restart shared channels  Y Y=Yes, N=No

Channel listener
Inbound disposition . . . Q G=Group, Q=Qmgr
Transport type . . . . . _ L=LU6.2, T=TCP/IP

Port number (TCP/IP) . . . _____
IP address (TCP/IP) . . . ________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 110. Zastavení řízení funkce

Vyberte funkci typu 1 (inicializátor kanálu) a stiskněte klávesu Enter.

Inicializátor kanálu čeká na zastavení všech spuštěných kanálů v klidovém režimu, než se zastaví.

Poznámka: Jsou-li některé kanály přijímači nebo žadatelovými kanály, které jsou spuštěny, ale nejsou aktivní, požadavek na zastavení vydaný na přijímač nebo iniciátor kanálu odesilatele způsobí okamžité zastavení.

Pokud však zprávy procházejí, inicializátor kanálu čeká na dokončení aktuální dávky zpráv, než se zastaví.

z/OS Spuštění modulu listener kanálu

Přijímač kanálů můžete spustit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li spustit modul listener kanálu pomocí příkazů MQSC, použijte příkaz START LISTENER.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	6 (Začátek)
Typ objektu	SYSTEM
Název	Prázdný

Zobrazí se panel Start a System Function (viz Obrázek 109 na stránce 881).

Vyberte typ funkce 2 (modul listener kanálu). Vyberte volbu Příchozí odebrání. Vyberte typ přenosu. Je-li typ transportu L, vyberte název LU. Je-li typ transportu T, vyberte číslo portu a (volitelně) IP adresu. Stiskněte klávesu Enter.

Poznámka: Pro modul listener protokolu TCP/IP můžete spustit více kombinací portu a adresy IP.

z/OS *Zastavení modulu listener kanálu*

Přijímač kanálů můžete zastavit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zastavit modul listener kanálu pomocí příkazů MQSC, použijte příkaz STOP LISTENER.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	7 (Zastavit)
Typ objektu	SYSTEM
Název	Prázdný

Zobrazí se panel Zastavit systém System Function (viz Obrázek 110 na stránce 882).

Vyberte typ funkce 2 (modul listener kanálu). Vyberte volbu Příchozí odebrání. Vyberte typ přenosu. Je-li typ transportu 'T', vyberte číslo portu a (volitelně) adresu IP. Stiskněte klávesu Enter.

Poznámka: V případě modulu listener protokolu TCP/IP můžete zastavit specifické kombinace portu a adresy IP nebo můžete zastavit všechny kombinace.

z/OS *Spuštění kanálu*

Kanál můžete spustit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li spustit kanál pomocí příkazů MQSC, použijte START CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	6 (Začátek)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Spustit kanál. Text na panelu vysvětluje, jak použít panel:

```
Start a Channel

Select disposition, then press Enter to start channel.


Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
S=Shared on MQ25
A=Shared on any queue manager









Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 111. Spuštění kanálu

Vyberte dispozice instance kanálu a na tom, který správce front 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. Pokusy o spuštění druhé instance kanálu selžou.

Spustíte-li kanál tímto způsobem, platí pro daný kanál následující pravidla:

- Kanál můžete zastavit z libovolného správce front ve skupině sdílení front. Můžete ji zastavit i v případě, že inicializátor kanálu, na kterém byla spuštěna, není spuštěna v době, kdy jste vydali požadavek na zastavení kanálu. Když je kanál zastaven, můžete jej restartovat uvedením dispozice = S (CHLDISP (FIXSHARED)) na stejném nebo jiném inicializátoru kanálu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Nachází-li se kanál ve stavu spuštění nebo opakování, můžete jej restartovat zadáním dispozice = S (CHLDISP (FIXSHARED)) na stejném nebo jiném inicializátoru kanálu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Kanál je způsobilý ke spuštění, když přejde do neaktivního stavu. Sdílené kanály, které spouštěč jsou spuštěny vždy, mají sdílenou dispozici (CHLDISP (SHARED)).
- Kanál je způsobilý ke spuštění s CHLDISP (FIXSHARED), na libovolném inicializátoru kanálu, když přejde do neaktivního stavu. Můžete jej také spustit zadáním dispozice = A (CHLDISP (SHARED)).
- Kanál není obnoven žádným jiným inicializačním kanálem kanálu ve skupině sdílení front, pokud inicializátor kanálu, ve kterém byla spuštěna, je zastaven pomocí příkazu SHARED (RESTART) nebo při nestandardním ukončení inicializátoru kanálu. Kanál je obnoven pouze v případě, že inicializátor kanálu, na kterém byl spuštěn, bude znovu spuštěn. Tím se zastaví pokusy o zotavení kanálu, které byly předány ostatním inicializátoru kanálu ve skupině sdílení front, které by se přidaly do jejich pracovní zátěže.

z/OS *Testování kanálu*

Kanál můžete testovat pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li testovat kanál s použitím příkazů MQSC, použijte příkaz PING CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	5 (Provést)
Typ objektu	SENDER, SERVER, nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu kanálu.

Zobrazí se panel Provést funkci kanálu. Text na panelu vysvětluje, jak použít panel:

```
Perform a Channel Function

Select function type, complete fields, then press Enter.


Function type . . . . . _   1. Reset  3. Resolve with commit
2. Ping  4. Resolve with backout

Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
S=Shared on MQ25
A=Shared on any queue manager

Sequence number for reset . . 1     1 - 999999999
Data length for ping . . . . 16   16 - 32768



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 112. Testování kanálu

Vyberte typ funkce 2 (příkaz ping).

Vyberte dispozice kanálu, pro který má být test proveden, a na kterém má být testován správce front.

Délka dat je na počátku nastavena na 16. Změňte jej, pokud chcete a stiskněte klávesu Enter.

z/OS *Resetování pořadových čísel zpráv pro kanál*

Pořadová čísla zpráv pro kanál můžete resetovat pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li resetovat pořadová čísla kanálů pomocí příkazů MQSC, použijte RESET CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	Hodnota
Akce	5 (Provést)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu kanálu.

Zobrazí se panel Provedení funkce kanálu (viz Obrázek 112 na stránce 885).

Vyberte typ funkce 1 (reset).

Vyberte dispozice kanálu, pro který má být proveden reset, a na kterém má být proveden správce front.

Pole **Pořadové číslo** je na počátku nastaveno na hodnotu jedna. Změňte tuto hodnotu, pokud chcete, a stiskněte klávesu Enter.

z/OS *Vyřešení nejistých zpráv na kanálu*

Pochybné zprávy na kanálu můžete vyřešit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li vyřešit nejisté zprávy na kanálu pomocí příkazů MQSC, použijte RESOLVE CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	5 (Provést)
Typ objektu	SENDER, SERVER, nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Provedení funkce kanálu (viz Obrázek 112 na stránce 885).

Vyberte typ funkce 3 nebo 4 (interprete s potvrzením nebo vyřazováním). (Další informace viz “Zacházení s nejistými kanály” na stránce 210 .)

Vyberte dispozice kanálu, pro který se má provést rozlišení a který správce front má být proveden. Stiskněte klávesu Enter.

z/OS *Zastavení kanálu*

Kanál můžete zastavit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zastavit kanál pomocí příkazů MQSC, použijte příkaz STOP CHANNEL.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	7 (Zastavit)
Typ objektu	typ kanálu (například SENDER) nebo CHANNEL
Název	CHANNEL.TO.USE
Dispozice	Dispozice objektu.

Zobrazí se panel Zastavení kanálu. Text na panelu vysvětluje, jak použít panel:

```
Stop a Channel

Complete fields, then press Enter to stop channel.


Channel name . . . . . : CHANNEL.TO.USE
Channel type . . . . . : SENDER
Description . . . . . : Description of CHANNEL.TO.USE


Disposition . . . . . P   P=Private on MQ25
A=Shared on any queue manager

Stop mode . . . . . 1   1. Quiesce  2. Force
Stop status . . . . . 1   1. Stopped  2. Inactive

Queue manager . . . . . _________________________________________________
Connection name . . . . . _________________________________________________



Command ===> ____________________________________________________________
F1=Help   F2=Split   F3=Exit   F9=SwapNext F10=Messages F12=Cancel
```

Obrázek 113. Zastavení kanálu

Vyberte dispozice kanálu, pro který má být zastaveno zastavení a na kterém má být zastaven správce front.

Zvolte režim zastavení, který požadujete:

Uvést do klidového stavu
Kanál se zastaví po dokončení aktuální zprávy a poté je dávka ukončena, i když nebyla dosažena hodnota velikosti dávky a zprávy již čekají na přenosovou frontu. Nejsou spuštěny žádné nové dávky. Tento režim je výchozí.

Vynutit
Kanál se zastaví okamžitě. Pokud probíhá zpracování dávky zpráv, může dojít k situaci 's nejistým stavem'.

Vyberte správce front a název připojení pro kanál, který chcete zastavit.

Vyberte stav, který požadujete:

Zastaveno
Kanál se automaticky nerestartuje a musí být restartován ručně. Tento režim je výchozí, není-li zadán žádný správce front nebo název připojení. Je-li uveden název, není to povoleno.

Neaktivní
Kanál se automaticky restartuje, je-li to nutné. Tento režim je výchozí, je-li zadán správce front nebo název připojení.

Stisknutím klávesy Enter zastavíte kanál.

Další informace viz “Zastavení a uvedení kanálů do klidového stavu” na stránce 208. Informace o restartování zastavených kanálů viz “Restartování zastavených kanálů” na stránce 210.

Poznámka: Je-li sdílený kanál ve stavu opakování a inicializátor kanálu, na kterém byl spuštěn, není spuštěn, je na správci front, ve kterém byl zadán příkaz, odeslán požadavek STOP pro kanál.

z/OS *Zobrazení stavu kanálu*

Stav kanálu můžete zobrazit pomocí příkazů MQSC, nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit stav kanálu nebo sady kanálů pomocí příkazů MQSC, použijte příkaz DISPLAY CHSTATUS.

Poznámka: Zobrazení informací o stavu kanálu může nějakou dobu trvat, máte-li mnoho kanálů.

Při použití operací a ovládacích panelů na panelu Seznam kanálů (viz téma Obrázek 106 na stránce 878) je pro každý kanál zobrazen souhrn stavu kanálu následovně:

INACTIVE	Nejsou aktivní žádná připojení
stav	Jedno připojení je aktivní
nnn stav	Více než jedno připojení je aktuální a všechna aktuální připojení mají stejný stav
nnn CURRENT	Více než jedno připojení je aktuální a aktuální připojení nemají všechny stejný stav.
Prázdný	IBM MQ nemůže určit, kolik připojení je aktivních (například, protože inicializátor kanálu není spuštěn)
	Poznámka: U objektů kanálu s dispozicí GROUP není zobrazen žádný stav.

kde *nnn* je počet aktivních připojení a *stav* je jeden z následujících:

Inicializovat	INICIALIZACE
BIND	Vazba
START	SPOUŠTĚNÍ
RUN	RUNNING
STOP	ZASTAVOVÁNÍ nebo ZASTAVENO
RETRY	Opakovaný pokus
REQST	Zpracování požadavků

Chcete-li zobrazit další informace o stavu kanálu, stiskněte klávesu Stav (F11) na kanálu seznamu nebo obrazovky nebo změňte panely kanálu a zobrazí se panel Seznam kanálů-Aktuální stav (viz Obrázek 114 na stránce 888).

```
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 114. Výpis připojení kanálů

Hodnoty stavu jsou následující:

Inicializovat	INICIALIZACE

BIND	Vazba
START	SPOUŠTĚNÍ
RUN	RUNNING
STOP	ZASTAVOVÁNÍ nebo ZASTAVENO
RETRY	Opakovaný pokus
REQST	Zpracování požadavků
POCHYBNÉ	ZASTAVENO a INDOUBT (YES)

Další informace viz “Stavy kanálů” na stránce 201.

Můžete stisknout klávesu F11 , abyste zobrazili podobný seznam připojení kanálů s uloženým stavem; stiskněte klávesu F11 , abyste se vrátili zpět na aktuální seznam. Uložený stav se neuplatní, dokud nebude na kanálu přenesena alespoň jedna dávka zpráv.

Použijte aktivační kód 1 nebo lomítko (/) pro výběr připojení a stiskněte klávesu Enter. Zobrazí se panely Zobrazit aktuální stav připojení kanálu.

z/OS *Zobrazení kanálů klastru*

Kanály klastru můžete zobrazit pomocí příkazů MQSC nebo pomocí operací a řídicích panelů.

Chcete-li zobrazit všechny kanály klastru, které byly definovány (explicitně nebo s použitím automatické definice), použijte příkaz MQSC, DISPLAY CLUSQMGR.

Pomocí operací a řídicích panelů, počínaje počátečním panelem, vyplňte tato pole a stiskněte klávesu Enter:

Pole	**Hodnota**
Akce	1 (Seznam nebo zobrazení)
Typ objektu	CLUSCHL
Název	*

Zobrazí se panel jako obrázek Obrázek 115 na stránce 890, v němž informace pro každý kanál klastru zaujímají tři řádky a obsahují názvy jeho kanálů, klastrů a správců front. Pro odesílací kanály klastru se zobrazí celkový stav.

```
List Cluster queue manager Channels - MQ25    Row 1 of 9

Type action codes, then press Enter. Press F11 to display connection status.
1=Display  5=Perform  6=Start  7=Stop

Channel name     Connection name                State
Type     Cluster name                  Suspended
Cluster queue manager name            Disposition
<>   *                        -    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 115. Zobrazení seznamu kanálů klastru

Chcete-li zobrazit úplné informace o jednom nebo více kanálech, zapište kód akce 1 proti jejich jménům a stiskněte klávesu Enter. Použijte kódy akce 5, 6 nebo 7 k provedení funkcí (jako např. ping, resolve a reset) a spuštění nebo zastavení kanálu klastru.

Chcete-li zobrazit další informace o stavu kanálu, stiskněte klávesu Stav (F11).

z/OS *Příprava produktu IBM MQ for z/OS k použití funkce produktu zEnterprise Data Compression Express*

Prostředek produktu zEnterprise Data Compression (zEDC) Express je k dispozici pro určité modely počítačů se systémem IBM Z , počínaje verzí IBM zEC12 GA2, s použitím minimální úrovně z/OS produktu z/OS 2.1.

Další informace viz zEnterprise Data Compression (zEDC) .

Požadavky

Pro IBM z15 a později byla funkce produktu zEnterprise Data Compression (zEDC) Express přesunuta z volitelné funkce v zásuvce I/O PCIe na hardwarovém systému, aby byla na čipu jako integrovaný akcelerátor pro zEDC. S touto změnou se aktualizují předpoklady konfigurace a jsou závislé na vašem hardwarovém systému.

IBM z15 nebo vyšší

V závislosti na úrovni operačního systému z/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 pozdější neexistují žádné požadavky na hardware. Integrované akcelerátor pro řešení zEDC v těchto systémech poskytuje vestavěnou akceleraci dat, takže samostatný adaptér již není zapotřebí.

IBM zEC12 GA2 až IBM z14

Váš systém musí mít také tyto požadavky:

- Adaptér zEDC Express ® instalovaný v zásuvkách I/O PCIe na hardwarovém systému.
- Schopnost softwaru zEDC (volitelná komponenta naiv-for) musí být povolena v členu knihovny parametrů IFAPRDxx.

Postup

IBM zEC12 GA2 až IBM z14

Ujistěte se, že ID uživatele iniciátoru kanálu má oprávnění READ pro FPZ.ACCELERATOR.COMPRESSION ve třídě FACILITY CLASS produktu RACF nebo ekvivalent v externím správci zabezpečení (ESM), který váš podnik používá.

Upozornění: Nepožaduje se pro IBM z15 nebo novější.

IBM zEnterprise zEC12 GA2 nebo novější

Konfigurujte kanál s parametrem COMPMSG (ZLIBFAST) na konci odesílání i příjmu. Po konfiguraci je komprese zlib použita ke kompresi a dekomprimaci zpráv procházejících přes kanál.

Komprese se provádí v zEDC , pokud velikost dat, která mají být komprimována, je nad minimální prahovou hodnotou. Prahová hodnota je závislá na použitém hardwaru produktu IBM z.

- IBM zEC12 GA2 až IBM z14 má minimální prahovou hodnotu 4KB
- IBM z15 nebo pozdější má minimální prahovou hodnotu 1KB

Pro zprávy pod prahovou hodnotou je komprese nebo inflace prováděna v softwaru.

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 nutné, aby připojení bylo definováno a dostupné. Tento oddíl vysvětluje, jak definovat připojení.

DQM je prostředek vzdáleného řazení do fronty pro produkt IBM MQ. Poskytuje řídicí programy kanálu pro správce front, který tvoří rozhraní pro komunikační propojení. Tyto odkazy jsou kontrolovatelné systémovým operátorem. Definice kanálů, které jsou v držení distribuované správy front, používají tato připojení.

Vyberte si z jednoho z těchto dvou druhů komunikačních protokolů, které lze použít pro produkt z/OS:

- “Definování připojení TCP na systému z/OS” na stránce 892
- “Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS” na stránce 894

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Každá definice kanálu musí určovat pouze jeden protokol jako atribut přenosového protokolu (Typ transportu). Správce front může ke komunikaci použít více než jeden protokol.

Může se také stát, že bude užitečné se podívat na téma Příklad konfigurace- IBM MQ for z/OS . Pokud používáte skupiny sdílení front, prohlédněte si téma “Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front” na stránce 900.

Související pojmy

“Použití panelů a příkazů” na stránce 877
Ke správě DQM můžete použít příkazy MQSC, příkazy PCF nebo operace a ovládací panely.

“nastaveníIBM MQ for z/OS” na stránce 800

Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ for z/OS .

“Monitorování a řízení kanálů v systému z/OS” na stránce 875
Pomocí příkazů DQM a panelů můžete vytvořit, monitorovat a řídit kanály pro vzdálené správce front.

“Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front” na stránce 896
Pomocí pokynů v této části můžete konfigurovat distribuované řazení do front se skupinami sdílení front v systému IBM MQ for z/OS.

“Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front” na stránce 900
Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení zadané v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby připojení bylo definováno a k dispozici.

Související úlohy

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 871
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, je zde několik nastavení, které je třeba nakonfigurovat.

Název adresního prostoru TCP musí být zadán v datové sadě systémových parametrů protokolu TCP, *tcpip*.TCPIP.DATA. V datové sadě musí být zahrnut příkaz "TCPIPJOBNAME *TCPIP_proc*" .

Používáte-li bránu firewall, je třeba konfigurovat připojení produktu `allow` z inicializátoru kanálu k adresám v kanálech a ze vzdálených připojení do správce front.

Definice brány firewall obvykle konfiguruje odesílající adresu IP a port do cílové adresy IP a portu:

- Obraz produktu z/OS může mít více než jeden název hostitele a může být zapotřebí nakonfigurovat bránu firewall s více adresami hostitele jako zdrojovou adresou.

  Chcete-li zobrazit tyto názvy a adresy, můžete použít příkaz NETSTAT HOME.
- Inicializátor kanálu může mít několik modulů listener na různých portech, takže je třeba tyto porty nakonfigurovat.
- Používáte-li sdílený port pro skupinu sdílení front, je třeba také nakonfigurovat sdílený port.

Adresní prostor inicializátoru kanálu musí mít oprávnění ke čtení datové sady. Následující techniky lze použít pro přístup k vašim TCPIP.DATA datové sady, v závislosti na tom, jaký produkt a rozhraní TCP/IP používáte:

- Proměnná prostředí, RESOLERVER_CONFIG
- /etc/resolv.conf v systému souborů
- // SYSTCPD DD, příkaz
- // SYSTCPDD DD, příkaz
- *jobname/userid*.TCPIP.DATA
- SYS1.TCPPARMS(TCPDATA)
- *zapname*.TCPIP.DATA

Musíte také být opatrní, abyste správně zadali kvalifikátor vyšší úrovně pro TCP/IP.

Potřebujete vhodně nakonfigurovaný server DNS (Domain Name System) schopný jak překlad adres IP, tak překlad adres IP na překlad názvů.

Poznámka: Některé změny v konfiguraci vyhodnocovacího modulu vyžadují recyklování aplikací, které jej používají, například IBM MQ.

Další informace jsou uvedeny v následujících tématech:

- Základní systém TCP/IP
- z/OS UNIX System Services.

Každý kanál TCP při spuštění používá prostředky TCP; možná budete muset upravit následující parametry ve vašem PROFILE.TCPIP :

VELIKOST FONDU ABPOOLSIZE
Přidejte jeden z spuštěných kanálů TCP a jeden z nich.

CCBPOOLSIZE
Přidejte jeden každý spuštěný kanál TCP a jeden pro každý dispečer DQM, plus jeden.

VELIKOST DATABUFFERPOOLSIZE
Přidejte dva pro každý spuštěný kanál TCP plus jeden.

MAXFILEPROC
Řídí, kolik kanálů může každý dispečer v inicializátoru kanálu zpracovat.

Tento parametr je uveden ve členu BPXPRMxx SYSI.PARMLIB. Ujistěte se, že jste zadali dostatečně velkou hodnotu pro vaše potřeby.

Inicializátor kanálu je ve výchozím nastavení schopen pouze vazby na adresy IP přidružené k zásobníku uvedenému v atributu správce front TCPNAME. Chcete-li povolit inicializátoru kanálu komunikovat s použitím dalších zásobníků TCP/IP na systému, změňte atribut správce front TCPSTACK na hodnotu MULTIPLE.

V 9.1.4 MQ Adv. CD Na kanál zpráv používající protokol TCP/IP lze poukázat na IBM Aspera fasp.io Gateway, který poskytuje rychlý tunel TCP/IP, který může výrazně zvýšit propustnost sítě. Správce front spuštěný na libovolné oprávněné platformě CD se může připojit prostřednictvím Aspera gateway. Samotná brána je implementována v systému Red Hat nebo Ubuntu Linux. Viz Definování Aspera gateway připojení na Linux.

Související pojmy

“Odesílání: Konec” na stránce 893
Na odesílajícím konci připojení TCP/IP existuje několik nastavení, které je třeba nakonfigurovat.

“Příjem na TCP” na stránce 894
Na přijímajícím konci připojení TCP/IP je zde několik nastavení, které lze konfigurovat.

“Použití volby nevyřízených požadavků na modul listener TCP” na stránce 894
Při příjmu v protokolu TCP/IP je nastaven maximální počet neprovedených požadavků na připojení. Tyto nevyřízené požadavky mohou být považovány za *nevyřízené požadavky* požadavků čekajících na portu TCP/IP pro modul listener, aby přijal požadavek.

z/OS *Odesílání: Konec*
Na odesílajícím konci připojení TCP/IP existuje několik nastavení, které je třeba nakonfigurovat.

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 tvaru IPv4 (například 127.0.0.1) nebo v hexadecimální formě IPv6 (například 2001:DB8:0:0:0:0:0:0). Je-li název připojení název hostitele, je požadován server názvů TCP pro převedení názvu hostitele na adresu hostitele TCP. (Tento požadavek je funkce protokolu TCP, nikoli IBM MQ.)

Na zahajovacím konci připojení (typy kanálů odesílatele, žadatele a serveru) je možné poskytnout volitelné číslo portu pro připojení, například:

Název připojení
192.0.2.0(1555)

V tomto případě se iniciující ukončení pokusí o připojení k přijímajícímu programu naslouchajícího na portu 1555.

Poznámka: Je-li zadáno volitelné číslo portu, použije se výchozí číslo portu 1414.

Inicializátor kanálu může použít libovolný zásobník TCP/IP, který je aktivní a dostupný. Inicializátor kanálu standardně sváže odchozí kanály s výchozí adresou IP pro zásobník TCP/IP, pojmenovaný v atributu

správce front TCPNAME. Chcete-li se připojit přes jiný zásobník, musíte uvést buď název hostitele, nebo adresu IP zásobníku v atributu LOCLADDR kanálu.

z/OS *Příjem na TCP*

Na přijímajícím konci připojení TCP/IP je zde několik nastavení, které lze konfigurovat.

Přijímající kanály jsou spuštěny jako odpověď na požadavek spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Tento program listener můžete spustit pomocí příkazu START LISTENER nebo pomocí operací a řídicích panelů.

Ve výchozím nastavení:

- Program TCP Listener používá port 1414 a naslouchá na všech adresách, které jsou dostupné pro zásobník TCP.
- Moduly listener protokolu TCP/IP se mohou vázat pouze na adresy přidružené k zásobníku TCP/IP jmenovanému v atributu správce front TCPNAME.

Chcete-li spustit listenery pro jiné adresy nebo všechny dostupné zásobníky TCP, nastavte atribut správce front TCPSTACK na 'MULTIPLE'.

Program modulu listener TCP můžete spustit tak, aby naslouchal pouze na určité adrese nebo názvu hostitele, zadáním IPADDR v příkazu START LISTENER. Další informace viz Moduly listener.

z/OS *Použití volby nevyřízených požadavků na modul listener TCP*

Při příjmu v protokolu TCP/IP je nastaven maximální počet neprovedených požadavků na připojení. Tyto nevyřízené požadavky mohou být považovány za *nevyřízené požadavky* požadavků čekajících na portu TCP/IP pro modul listener, aby přijal požadavek.

Výchozí hodnota nevyřízených požadavků listeneru na z/OS je 10000. Pokud jsou tyto hodnoty nahromadění nevyřízených požadavků, je připojení TCP/IP zamítnuto a kanál se nemůže spustit.

V případě kanálu MCA se výsledkem tohoto výsledku v kanálu stane stav ZOPAKOVAT a později se znovu pokusí o připojení.

V případě připojení klienta obdrží klient kód příčiny MQRC_Q_MGR_NOT_AVAILABLE z objektu MQCONN a později se může připojení pokusit o zopakování připojení.

z/OS *Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS*

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

Nastavení APPC/MVS

Každá instance inicializátoru kanálu musí mít název jednotky LU, kterou má být nadefinován pro APPC/MVS, ve členu APPCPMxx SYS1.PARMLIB, jako v následujícím příkladu:

```
LUADD ACBNAME( luname ) NOSCHED TPDATA(CSQ.APPCTP)
```

luname je název logické jednotky, která má být použita. NOSCHED je povinný; TPDATA se nepoužije. Pro člen ASCHPMxx nebo pro datovou sadu profilu APPC/MVS TP nejsou nutná žádná doplnění.

Datová sada bočních informací musí být rozšířena, aby definovala připojení použitá aplikací DQM. Podrobné informace o tom, jak postupovat při použití obslužného programu ATBSDFMU, najdete v dodané ukázce CSQ4SIDE . Chcete-li získat podrobnosti o hodnotách TPNAME, prohlédněte si následující tabulku, kde získáte informace:

Tabulka 65. Nastavení na lokálním systému z/OS pro vzdálenou platformu správce front	
Vzdálená platforma	**TPNAME**
z/OS nebo MVS	Tentýž jako TPNAME v odpovídajících informacích o vzdáleném správci front.
IBM i	Stejné jako porovnávací hodnota v záznamu směrování v systému IBM i .
Systémy UNIX and Linux	Tentýž jako TPNAME v odpovídajících informacích o vzdáleném správci front.
Windows	Jak je uvedeno v příkazu Windows Spustit modul listener nebo na nezvolnitelném transakčním programu, který byl definován pomocí volby TpSetup na serveru Windows.

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

Další informace o definicích modulů VTAM, které mohou být vyžadovány, naleznete v příručce *Multiplatform APPC Configuration Guide* .

V prostředí, ve kterém správce front komunikuje pomocí APPC se správcem front ve stejném nebo v jiném systému z/OS , zkontrolujte, zda definice VTAM pro komunikační LU určuje SECACPT (ALREADYV), nebo že existuje profil RACF APPCLU pro připojení mezi jednotkami LU, který uvádí CONVSEC (ALREADYV).

Příkaz z/OS VARY ACTIVE musí být před pokusem o spuštění příchozí nebo odchozí komunikace vydán proti jednotkám LU Base a modulu listener.

Upozornění: Kromě nastavení APPC je třeba zadat následující příkaz:

```
ALTER QMGR LUNAME(luname)
```

a restartujte inicializátor kanálu.

Další informace viz LUNAME .

Související pojmy

“Připojování k LU 6.2” na stránce 895
Chcete-li se připojit k LU 6.2, je třeba nakonfigurovat několik nastavení.

“Příjem na LU 6.2” na stránce 895
Pro přijetí na LU 6.2existuje několik nastavení, které je třeba nakonfigurovat.

z/OS *Připojování k LU 6.2*

Chcete-li se připojit k LU 6.2, je třeba nakonfigurovat několik nastavení.

Pole názvu připojení (CONNAME) v definici kanálu musí být nastaveno na symbolický název cíle, jak je uvedeno v datové sadě informací o připojení pro APPC/MVS.

Název jednotky LU, který má být použit (definovaný pro parametr APPC/MVS, jak je popsáno výše), musí být také zadán v parametrech inicializátoru kanálu. Musí být nastaven na stejnou logickou jednotku, která je používána pro příjem posluchače.

Inicializátor kanálu používá volbu APPC/MVS "SECURITY (SAME)" , takže se jedná o ID uživatele adresního prostoru iniciátoru kanálu, který se používá pro odchozí přenosy, a je předložen příjemci.

z/OS *Příjem na LU 6.2*

Pro přijetí na LU 6.2existuje několik nastavení, které je třeba nakonfigurovat.

Příjem MCA se spouští jako odezva na požadavek spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn program listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Program modulu listener je server APPC/MVS. Spustíte ji pomocí příkazu START LISTENER nebo pomocí operací a řídicích panelů. Je třeba určit název jednotky LU, který má být použit se symbolickým názvem místa

určení definovaným v datové sadě informací o připojení. Identifikovaná lokální LU musí být stejná jako ta, která se používá pro odchozí přenosy, jak je nastaveno v parametrech inicializátoru kanálu.

z/OS Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front

Pomocí pokynů v této části můžete konfigurovat distribuované řazení do front se skupinami sdílení front v systému IBM MQ for z/OS.

Příklad konfigurace pomocí skupin sdílení front naleznete v tématu Příklad konfigurace- IBM MQ for z/OS pomocí skupin sdílení front. Příklad plánování kanálu zpráv pomocí skupin sdílení front naleznete v tématu Příklad plánování kanálů zpráv pro produkt z/OS s použitím skupin sdílení front.

Chcete-li povolit distribuované řazení do front se skupinami sdílení front, je třeba vytvořit a konfigurovat následující komponenty:

- Moduly listener LU 6.2 a TCP/IP
- Přenosové fronty a spuštění
- Agenti kanálů zpráv
- Fronta synchronizace

Poté, co jste vytvořili komponenty potřebné k nastavení komunikace, prohlédněte si téma “Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front” na stránce 900.

Informace o tom, jak monitorovat a řídit kanály při používání skupin sdílení front, viz “Monitorování a řízení kanálů v systému z/OS” na stránce 875.

Informace o konceptech a výhodách skupiny sdílení front naleznete v následujících oddílech.

Třída služeb

Sdílená fronta je typem lokální fronty, která nabízí jinou třídu služeb. Zprávy v rámci sdílené fronty jsou uloženy v prostředku CF (coupling facility), který jim umožňuje přístup ke všem správcům front ve skupině sdílení front. Zpráva ve sdílené frontě musí být zpráva o délce nejvýše 100 MB.

Generické rozhraní

Skupina sdílení front má generické rozhraní, které umožňuje, aby síť prohlížela skupinu jako jedinou entitu. Toto zobrazení je dosaženo pomocí jediné generické adresy, kterou lze použít pro připojení k libovolnému správci front v rámci skupiny.

Každý správce front ve skupině sdílení front naslouchá příchozím požadavkům relací na adrese, která je logicky vztak k generické adrese. Další informace viz “Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front” na stránce 897.

Začátek vyrovnaného kanálu

Sdílenou přenosovou frontu může obsloužit odchozí kanál, který je spuštěn na libovolném inicializátoru kanálu ve skupině sdílení front. Spuštění kanálu s vyrovnáním zátěže určuje, kde je zacílen příkaz ke spuštění kanálu. Je zvolen vhodný inicializátor kanálu, který má přístup k nezbytným komunikačním subsystémem. Například kanál definovaný s TRPTYPE (LU6.2) nemůže být spuštěn na inicializátoru kanálu, který má pouze přístup k subsystému TCP/IP.

Volba inicializátoru kanálu závisí na zatížení kanálu a na hlavní místnosti iniciátoru kanálu. Zatížení kanálu je počet aktivních kanálů vyjádřený jako procentní podíl maximálního počtu povolených aktivních kanálů, jak je definováno v parametrech inicializátoru kanálu. Místnost je rozdíl mezi počtem aktivních kanálů a maximálním přípustným počtem kanálů.

Příchozí sdílené kanály mohou být vyrovnány do skupiny sdílení front použitím generické adresy, jak je popsáno v tématu “Moduly listener LU 6.2 a TCP/IP pro skupiny sdílení front” na stránce 897.

Obnova sdíleného kanálu

V následující tabulce jsou uvedeny typy selhání se sdílenými kanály a způsob zpracování jednotlivých typů.

Typ selhání:	Co se děje:
Selhání komunikačního subsystému inicializátoru kanálu	Kanály závislé na komunikačním subsystému vstupují do kanálu znovu a jsou restartovány u příslušného inicializátoru kanálu se skupinou sdílení front pomocí příkazu ke spuštění s vyrovnáním zátěže.
Selhání inicializátoru kanálu	Inicializátor kanálu selže, ale přidružený správce front zůstane aktivní. Správce front monitoruje selhání a zahajuje zpracování zotavení.
Selhání správce front	Dojde k selhání správce front (selhání přidruženého iniciátoru kanálu). Ostatní správci front v rámci skupiny sdílení front tuto událost sledují a iniciují zotavení typu peer.
Selhání sdíleného stavu	Informace o stavu kanálu jsou uloženy v produktu Db2, takže ztráta konektivity k produktu Db2 se stane selháním, pokud dojde ke změně stavu kanálu. Spuštěné kanály mohou provádět provoz bez přístupu k těmto prostředkům. Při neúspěšném přístupu k produktu Db2se kanál znovu pokusí o opakování.

Zpracování zotavení sdíleného kanálu pro systém, který selhal, vyžaduje připojení k produktu Db2 , které má být k dispozici v systému spravujícím obnovu k načtení stavu sdíleného kanálu.

Kanály klienta

Kanály připojení klienta mohou těžit z vysoké dostupnosti zpráv ve skupinách sdílení front, které jsou připojeny ke generickému rozhraní místo toho, aby byly připojeny 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 800
Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ for z/OS .

“Klastry a skupiny sdílení front” na stránce 899
Sdílenou frontu můžete zpřístupnit pro klastr v jediné definici. Chcete-li tak učinit, zadejte při definování sdílené fronty název klastru.

“Kanály a serializace” na stránce 899
Během partnerské obnovy sdílené fronty zpráv kanálu zpráv, které zpracovávají zprávy ve sdílených frontách, serializuje jejich přístup k frontám.

Použití front v rámci skupiny

Související úlohy

“Konfigurace distribuovaných front” na stránce 171
Tento oddíl poskytuje podrobnější informace o mezikomunikaci mezi instalacemi produktu IBM MQ , včetně definice fronty, definice kanálu, spouštěče a procedur synchronizačních bodů.

“Nastavení komunikace s ostatními správci front v systému z/OS” na stránce 871
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*

Skupině LU 6.2 a posluchači TCP/IP naslouchají na adrese, která je logicky připojena ke generické adrese.

V případě modulu listener LU 6.2 je uvedená skupina LUGROUP mapována na generický prostředek VTAM přidružený ke skupině sdílení front. Příklad nastavení této technologie viz “Definování připojení LU6.2 pro produkt z/OS pomocí APPC/MVS” na stránce 894.

V případě modulu listener protokolu TCP/IP může být uvedený port připojen k obecné adrese jedním z následujících způsobů:

- Pro front-endový směrovač, jako je například IBM Network Dispatcher, jsou příchozí požadavky na připojení přesměrovány ze směrovače na členy skupiny sdílení front.
- Pro distributor prostředí sysplex protokolu TCP/IP je každý modul listener, který běží a naslouchá na konkrétní adrese, která je nastavena jako distribuovaná DVIPA, přidělen poměrům příchozích požadavků. Příklad nastavení této technologie naleznete v tématu Použití distributoru prostředí sysplex .

z/OS *Přenosové fronty a spuštění pro skupiny sdílení front*

Sdílená přenosová fronta se používá k ukládání zpráv před přesunutím ze skupiny sdílení front do cíle.

Jedná se o sdílenou frontu a je přístupná pro všechny správce front ve skupině sdílení front.

Spouątění

Spuštěná sdílená fronta může vygenerovat více než jednu zprávu spouštěče pro splněnou podmínku spouštěče. Pro každou lokální inicializační frontu definovanou ve správci front v rámci skupiny sdílení front přidružené ke spuštěné sdílené frontě je vygenerována jedna zpráva spouštěče.

Pro distribuované řazení do fronty obdrží každý iniciátor kanálu zprávu spouštěče pro splněnou podmínku spouštěče sdílené přenosové fronty. Ale pouze jeden iniciátor kanálu skutečně zpracovává spuštěný start a ostatní selžou bezpečně. Spuštěný kanál je poté spuštěn s vyrovnáním zátěže (viz “Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front” na stránce 896). který se spustí ke spuštění kanálu `QSG.TO.QM2`. Chcete-li vytvořit sdílenou přenosovou frontu, použijte příkazy IBM MQ (MQSC), jak je uvedeno v následujícím příkladu:

```
DEFINE QLOCAL(QM2) DESCR('Transmission queue to QM2') +
USAGE(XMITQ) QSGDISP(SHARED) +
CFSTRUCT(APPLICATION1) INITQ(SYSTEM.CHANNEL.INITQ) +
TRIGGER TRIGDATA(QSG.TO.QM2)
```

Poznámka: Je-li sdílená fronta nastavena na spuštění a připojení k prostředku Coupling Facility, který je hostitelem sdílené fronty, může být generována událost spouštěče a zpráva vložena do inicializační fronty. K tomu může dojít i v případě, kdy nebyla do původní sdílené fronty nastavena žádná zpráva pro spuštění. To je způsobeno přeznačením bitů podle makra IXLVECTR, jak je dokumentováno v Vektoru oznámení seznamu.

z/OS *Agenti kanálů zpráv pro skupiny sdílení front*

Kanál může být na inicializátoru kanálu spuštěn pouze v případě, že má přístup k definici kanálu pro kanál s tímto názvem.

Agent oznamovacího kanálu je program IBM MQ , který řídí odesílání a příjem zpráv. Agenti kanálu zpráv přesouvají zprávy z jednoho správce front do jiného; na každém konci kanálu je jeden agent kanálu zpráv.

Definice kanálu může být definována jako soukromá pro správce front nebo je uložena ve sdíleném úložišti a je k dispozici kdekoli (definice skupiny). To znamená, že kanál definovaný skupinou je k dispozici u všech inicializátoru kanálu ve skupině sdílení front.

Poznámka: Soukromá kopie definice skupiny může být změněna nebo odstraněna.

Chcete-li vytvořit definice kanálů skupiny, použijte příkazy IBM MQ (MQSC), jak je uvedeno v následujících příkladech:

```
DEFINE CHL(QSG.TO.QM2) CHLTYPE(SDR) +
TRPTYPE(TCP) CONNAME(QM2.MACH.IBM.COM) +
XMITQ(QM2) QSGDISP(GROUP)
```

```
DEFINE CHL(QM2.TO.QSG) CHLTYPE(RCVR) TRPTYPE(TCP) +
QSGDISP(GROUP)
```

Existují dvě perspektivy, ze kterých se můžete podívat na agenty kanálů zpráv použité pro distribuované řazení do front se skupinami sdílení front:

Příchozí

Příchozí kanál je sdílený kanál, je-li připojen ke správci front prostřednictvím skupinového modulu listener. Je připojen buď pomocí generického rozhraní do skupiny sdílení front, a poté přesměrován na správce front v rámci skupiny nebo zacílený na port skupiny specifického správce front nebo název-lume používaný modulem listener skupiny.

Odchozí

Odchozí kanál je sdílený kanál, pokud přesouvá zprávy ze sdílené přenosové fronty. V ukázkových příkazech je odesílací kanál `QSG.TO.QM2` sdíleným kanálem, protože jeho přenosová fronta QM2 je definována s QSGDISP (SHARED).

z/OS *Fronta synchronizace pro skupiny sdílení front*

Sdílené kanály mají svou vlastní sdílenou synchronizační frontu s názvem SYSTEM.QSG.CHANNEL.SYNCQ.

Tato synchronizační fronta je přístupná pro všechny členy skupiny sdílení front. (Soukromé kanály nadále používají soukromou synchronizační frontu. Viz “Definování objektů IBM MQ” na stránce 874). To znamená, že kanál může být restartován v jiném správci front a instanci inicializátoru kanálu v rámci skupiny sdílení front v případě selhání komunikačního subsystému, inicializátoru kanálu nebo správce front. Další informace uvádí téma “Příprava produktu IBM MQ for z/OS for DQM se skupinami sdílení front” na stránce 896.

DQM se skupinami sdílení front vyžaduje, aby byla sdílená fronta k dispozici s názvem SYSTEM.QSG.CHANNEL.SYNCQ. Tato fronta musí být k dispozici, aby mohl být modul listener skupiny úspěšně spuštěn.

Pokud se modul listener skupiny nezdaří, protože fronta nebyla k dispozici, může být definována fronta a modul listener lze restartovat bez restartování inicializátoru kanálu. Nesdílené kanály nejsou ovlivněny.

Ujistěte se, že jste definovali tuto frontu pomocí INDXTYPE (MSGID). Tato definice zvyšuje rychlost, jakou lze přistupovat ke zprávám ve frontě.

z/OS *Klastry a skupiny sdílení front*

Sdílenou frontu můžete zpřístupnit pro klastr v jediné definici. Chcete-li tak učinit, zadejte při definování sdílené fronty název klastru.

Uživatelé v síti vidí sdílenou frontu jako hostitele každého správce front v rámci skupiny sdílení front. (Sdílená fronta není deklarována 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 “Konfigurace klastru správce front” na stránce 265.

z/OS *Kanály a serializace*

Během partnerské obnovy sdílené fronty zpráv kanálu zpráv, které zpracovávají zprávy ve sdílených frontách, serializuje jejich přístup k frontám.

Selže-li správce front ve skupině sdílení front v době, kdy agent kanálu zpráv pracuje s nepotvrzenými zprávami v jedné nebo více sdílených frontách, dojde k ukončení kanálu a přidruženého inicializátoru kanálu a k zotavení sdílené fronty bude pro správce front provedena operace partnerského serveru typu peer.

Vzhledem k tomu, že partnerská obnova sdílené fronty je asynchronní činnost, může se zotavení partnerského kanálu pokusit o restartování kanálu v jiné části skupiny sdílení front před dokončením

zotavení sdílené fronty typu peer. Pokud se tato událost stane, mohou být potvrzené zprávy zpracovány před tím, než se zprávy stále zotavují. Chcete-li se ujistit, že zprávy nejsou tímto způsobem zpracovány, agenti kanálu zpráv, kteří zpracovávají zprávy ve sdílených frontách, serializují jejich přístup k těmto frontám.

Pokus o spuštění kanálu, pro který stále probíhá obnova sdílené fronty zpráv, může vést k selhání. Bude vydána chybová zpráva oznamující, že zotavení probíhá, a kanál je uveden do stavu opakování. Jakmile je obnova typu peer správce front dokončena, kanál se může restartovat při následujícím opakování.

Pokus o RESOLVE, PING nebo DELETE kanálu může selhat ze stejného důvodu.

z/OS *Nastavení komunikace pro prostor IBM MQ for z/OS pomocí skupin sdílení front*

Je-li spuštěn kanál správy distribuovaných front, pokusí se použít připojení zadané v definici kanálu. Aby byl tento pokus úspěšný, je nezbytné, aby připojení bylo definováno a k dispozici.

Vyberte si z jednoho ze dvou typů komunikačního protokolu, který lze použít:

- TCP
- LU 6.2 až APPC/MVS

Může být užitečné se podívat na volbu Příklad konfigurace- IBM MQ for z/OS pomocí skupin sdílení front.

z/OS *Definování připojení TCP pro skupiny sdílení front*

Chcete-li definovat připojení TCP pro skupinu sdílení front, musí být nakonfigurovány určité atributy na odesílajícím a přijímajícím ukončení.

Informace o nastavení protokolu TCP naleznete v tématu “Definování připojení TCP na systému z/OS” na stránce 892.

Odesílání: Konec

Pole názvu připojení (CONNAME) v definici kanálu pro připojení k vaší skupině sdílení front musí být nastaveno na generické rozhraní skupiny sdílení front (viz Skupiny sdílení front). Další informace naleznete v tématu Použití distributoru prostředí sysplex.

Příjem na TCP pomocí skupiny sdílení front

Příjem sdílených programů kanálu je spuštěn jako odezva na požadavek na spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn modul listener ke zjištění příchozích síťových požadavků a spuštění přidruženého kanálu. Tento program listener můžete spustit pomocí příkazu START LISTENER, s použitím příchozí odebrání skupiny nebo pomocí operací a řídicích panelů.

Všechny listenery skupin ve skupině sdílení front musí naslouchat na stejném portu. Máte-li více než jeden inicializátor kanálu běžící na jednom obrazu MVS, můžete definovat virtuální IP adresy a spustit program TCP listener pouze na určité adrese nebo názvu hostitele zadáním IPADDR v příkazu START LISTENER. (Další informace viz START LISTENER.)

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 ukončení.

Informace o nastavení APPC/MVS naleznete v tématu Nastavení komunikace pro z/OS .

Připojování k APPC/MVS (LU 6.2)

Pole názvu připojení (CONNAME) v definici kanálu pro připojení k vaší skupině sdílení front musí být nastaveno na symbolický název cíle, jak je uvedeno v datové sadě informací o připojení pro APPC/MVS. Partnerská LU uvedená v tomto symbolickém cíli musí být generický název prostředku. Další informace najdete v tématu Definování do sítě pomocí generických prostředků.

Příjem na LU 6.2 pomocí generického rozhraní

Příjem sdílených MCA se spouští jako odezva na požadavek spuštění z odesílajícího kanálu. Chcete-li tak učinit, musí být spuštěn program skupinového modulu listener, který zjistí příchozí síťové požadavky a spustí přidružený kanál. Program modulu listener je server APPC/MVS. Spustíte ji pomocí příkazu START LISTENER, s použitím příchozí skupiny odebrání nebo pomocí operací a řídicích panelů. Je třeba určit název jednotky LU pro použití symbolického názvu místa určení definovaného v datové sadě informací o připojení. Další informace najdete v tématu Definování do sítě pomocí generických prostředků.

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 produkty IBM MQ a IMS pro spolupráci, je třeba provést následující úlohy:

- "Nastavení adaptéru IMS" na stránce 901
- "Nastavení mostu IMS" na stránce 908

Související pojmy

IBM MQ a IMS

"Použití IBM MQ s CICS" na stránce 909
Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge .

"Použití uživatelských procedur OTMA v adresáři IMS" na stránce 912
Toto téma použijte, chcete-li použít uživatelské procedury IMS Open Transaction Manager Access s produktem IBM MQ for z/OS.

Aplikace mostu IMS a IMS v systému IBM MQ for z/OS

Související úlohy

"Konfigurace správců front v systému z/OS" na stránce 795
Tyto pokyny použijte ke konfiguraci správců front v systému IBM MQ for z/OS.

Související odkazy

"Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services" na stránce 909
Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

z/OS Nastavení adaptéru IMS

Použití produktu IBM MQ v rámci struktury IMS vyžaduje adaptér IBM MQ - IMS (obecně nazývaný jako adaptér IMS).

Toto téma obsahuje informace o tom, jak lze adaptér IMS zpřístupnit pro subsystém IMS . Pokud nejste obeznámeni s přizpůsobením subsystému IMS , přečtěte si téma *Informace o produktu IMS v příručce IBM Documentation*.

Chcete-li zpřístupnit adaptér IMS aplikacím produktu IMS , postupujte takto:

1. Define IBM MQ to IMS as an external subsystem using the IMS external subsystem attach facility (ESAF).

   Viz "Definování IBM MQ na IMS" na stránce 903.

2. Do souboru JOBLIB nebo STEPLIB ve zřetězení JOBLIB nebo STEPLIB zahrňte do souboru JCL pro řídicí oblast IMS a pro všechny závislé oblasti, které se připojí k produktu IBM MQ (pokud není v LPA nebo seznamu odkazů), vložte zaváděcí knihovnu IBM MQ thlqual.SCSQAUTH do souboru JOBLIB nebo STEPLIB. Není-li vaše knihovna JOBLIB nebo STEPLIB autorizována, zahrňte ji do zřetězení DFSESL za knihovnu obsahující moduly IMS (obvykle IMS RESLIB).

   Zahrňte také thlqual.SCSQANLx (kde x je jazykový dopis).

   Je-li DFSESL přítomen, pak je třeba do zřetězení přidat SCSQAUTH a SCSQANLx nebo přidat do LNKLIST. Přidání do zřetězení STEPLIB nebo JOBLIB v souboru JCL není dostatečné.

3. Okopírujte program IBM MQ assembler CSQQDEFV z thlqual.SCSQASMS do uživatelské knihovny.
4. Dodaný program CSQQDEFV obsahuje jeden název subsystému CSQ1 identifikované jako výchozí s tokenem jazyka IMS (LIT) produktu MQM1. Tento název můžete uchovat pro testování a verifikaci instalace.

   Pro produkční subsystémy změňte hodnotu NAME=CSQ1 na své vlastní jméno podsystému, nebo použijte CSQ1. Podle potřeby můžete přidat další definice subsystému. Další informace o LITs najdete v tématu “Definování správců front IBM MQ na adaptér IMS” na stránce 906 .
5. Sestavte a propojte program za účelem vytvoření zaváděcího modulu CSQQDEFV. Pro sestavení přidejte do zřetězení SYSLIB knihovnu thlqual.SCSQMACS ; použijte parametr link-edit RENT. Tato hodnota je zobrazena v ukázkovém JCL v souboru thlqual.SCSQPROC(CSQ4DEFV).
6. Zahrňte uživatelskou knihovnu obsahující modul CSQQDEFV, který jste vytvořili ve zřetězení JOBLIB nebo STEPLIB v souboru JCL pro libovolnou závislou oblast, která se připojuje k produktu IBM MQ. Umístěte tuto knihovnu před objekt SCSQAUTH, protože modul SCSQAUTH má nastaven výchozí modul načítání. Pokud toto neuděláte, obdržíte uživatele 3041 abend od IMS.
7. Pokud adaptér IMS zjistí neočekávanou chybu IBM MQ , vyšle výpis paměti z/OS SNAP do názvu DD CSQSNAP a vydá aplikaci kód příčiny příčiny MQRC_UNEXPECTED_ERROR. Pokud příkaz CSQSNAP DD nebyl v kódu JCL oblasti závislé na IMS , nebude proveden žádný výpis paměti. Pokud k tomu dojde, můžete do JCL zahrnout příkaz CSQSNAP DD a znovu spustit aplikaci. Protože však některé problémy mohou být občasné, doporučuje se zahrnout příkaz CSQSNAP DD, abyste zachytili příčinu selhání v době, kdy k němu dojde.
8. Chcete-li použít dynamické volání IBM MQ (popsané v části Dynamicky volat stubu IBM MQ), sestavte dynamický stub, jak ukazuje Obrázek 116 na stránce 903.
9. Chcete-li použít monitor spouštěčů produktu IMS , definujte monitor spouštěčů produktu IMS CSQQTRMN a proveďte příkazy PSBGEN a ACBGEN. Viz téma “Nastavení monitoru spouštěčů IMS” na stránce 907.
10. Pokud používáte produkt RACF k ochraně prostředků ve třídě OPERCMDS, ujistěte se, že ID uživatele přidružené k adresnímu prostoru správce front produktu IBM MQ má oprávnění k vydání příkazu MODIFY pro libovolný systém IMS , ke kterému se může připojit.

```
//DYNSTUB EXEC PGM=IEWL,PARM='RENT,REUS,MAP,XREF'
//SYSPRINT DD  SYSOUT=*
//ACSQMOD  DD  DISP=SHR,DSN=thlqual.SCSQLOAD
//IMSLIB   DD  DISP=SHR,DSN=ims.reslib
//SYSLMOD  DD  DISP=SHR,DSN=private.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 116. Ukázka skriptu JCL pro propojení-úprava stubu dynamického volání

Související pojmy

IBM MQ a IMS

“Nastavení mostu IMS” na stránce 908

Most IBM MQ - IMS je volitelná komponenta, která umožňuje IBM MQ vstupu a výstupu do a z existujících programů a transakcí, které nejsou IBM MQ-enabled.

Aplikace mostu IMS a IMS v systému IBM MQ for z/OS

z/OS *Definování IBM MQ na IMS*

IBM MQ musí být definován pro řídicí oblast IMS a pro každou závislou oblast přistupujícího ke správci front IBM MQ . Chcete-li to provést, musíte v produktu IMSvytvořit člena subsystému (SSM).Knihovna PROCLIB a identifikujte SSM v příslušných regionech IMS .

Umístění položky člena subsystému do IMS.PROCLIB

Každá položka SSM v produktu IMS.PROCLIB definuje připojení z regionu produktu IMS k jinému správci front.

To name an SSM, concatenate the value (one to four alphanumeric characters) of the IMSID field of the IMS IMSCTRL macro with any name (one to four alphanumeric characters) defined by your site.

Jeden SSM může být sdílen všemi regiony IMS nebo může být definován specifický člen pro každý region. Tento člen obsahuje tolik položek, jako jsou připojení k externím subsystémům. Každá položka je záznam o délce 80 znaků.

Poziční parametry

Pole v této položce jsou:

```
SSN,LIT,ESMT,RTT,REO,CRC
```

kde:

SSN
Určuje název správce front produktu IBM MQ . Je to povinné a musí obsahovat jeden až čtyři znaky.

LIT
Určuje token jazykového rozhraní (LIT-Language Interface Token) dodaný produktu IMS. Toto pole je povinné, jeho hodnota se musí shodovat s hodnotou v modulu CSQQDEFV.

ESMIT
Uvádí tabulku modulu externího subsystému (ESMT). Tato tabulka určuje, které moduly příloh musí být načteny produktem IMS. CSQQESMT je požadovaná hodnota pro toto pole.

RTTŮV
Tato volba není podporována produktem IBM MQ.

REO
Uvádí volbu chyby regionu (REO), která se má použít, pokud aplikace IMS odkazuje na jiný než operační externí subsystém nebo pokud nejsou prostředky k dispozici při vytváření času podprocesu. Toto pole je volitelné a obsahuje jeden znak, který může být:

R
Předává návratový kód aplikaci, což označuje, že požadavek na služby IBM MQ selhal.

Q
Ukončí aplikaci s kódem nestandardního ukončení U3051, zálohuje aktivitu na poslední bod potvrzení, provede operaci PSTOP pro transakci a znovu odešle vstupní zprávu. Tato volba se používá pouze tehdy, když se aplikace IMS pokouší odkazovat na jiný než operační externí subsystém, nebo pokud nejsou prostředky k dispozici při vytváření času podprocesu.

IBM MQ a kódy příčiny jsou vráceny aplikaci, pokud se problém IBM MQ vyskytne, zatímco IBM MQ zpracovává požadavek; to znamená poté, co adaptér předal požadavek na IBM MQ.

A
Ukončí aplikaci s kódem abend U3047 a zahodí vstupní zprávu. Tato volba se používá pouze v případě, že aplikace IMS odkazuje na jiný než operační externí subsystém, nebo pokud jsou prostředky nedostupné při vytváření času podprocesu.

IBM MQ a kódy příčiny jsou vráceny aplikaci, pokud se problém IBM MQ vyskytne, zatímco IBM MQ zpracovává požadavek; to znamená poté, co adaptér předal požadavek na IBM MQ.

CRC
Tato volba může být uvedena, ale není použita IBM MQ.

Poznámka: Podrobné informace o všech pozičních parametrech najdete v tématu Jak jsou externí subsystémy zadány do systému IMS.

Příklad záznamu SSM je:

```
CSQ1,MQM1,CSQQESMT,,R,
```

kde:

CSQ1	Výchozí název subsystému, jak je dodáván s IBM MQ. Tento stav můžete změnit, aby vyhovoval vaší instalaci.
MQM1	Výchozí hodnota LIT, jak je dodána v CSQQDEFV.

CSQQESMT	Název modulu externího subsystému. Tuto hodnotu musíte použít.
R	Volba REO.

Parametry klíčových slov

Parametry IBM MQ lze zadat ve formátu klíčových slov. Parametr SST může mít hodnotu buď DB2 , nebo MQ. Podpora pro hodnotu MQ byla přidána do IMS 14. Použití podpory produktu MQ a příkaz subsystému IMS nyní zahrnuje hodnotu SST, ale jinak žádný významný efekt nemá. V případě potřeby lze i nadále používat hodnotu DB2 . Ostatní parametry jsou popsané v části Poziční parametrya jsou zobrazeny v následujícím příkladu:

```
SST=MQ,SSN=SYS3,LIT=MQM3,ESMT=CSQQESMT
```

kde:

SYS3	Název subsystému
MQM3	LIT, jak je uvedeno v CSQQDEFV
CSQQESMT	Název modulu externího subsystému

Uvedení parametru EXEC SSM

Uveďte parametr EXEC SSM ve spouštěcí proceduře řídicí oblasti IMS . Tento parametr uvádí jeden znak pro čtyřznakový název člena subsystému (SSM).

Uvedete-li SSM pro řídicí oblast IMS , jakýkoli závislý region spuštěný pod řídicí oblastí se může připojit ke správci front IBM MQ uvedenému v IMS.Člen PROCLIB uvedený v parametru SSM. IMS.Název členu PROCLIB je ID IMS (IMSID= *xxxx*) zřetězené s jedním až čtyřmi znaky zadanými v parametru EXEC SSM. ID IMS je parametr ID IMSmakra generování CTRL IMS.

Produkt IMS umožňuje definovat tolik externích připojení k subsystému, jak je požadováno. Pro různé správce front IBM MQ může být definováno více než jedno připojení. Všechna spojení typu IBM MQ musí být ve stejném systému z/OS . Pro závislou oblast můžete uvést závislý region SSM nebo použít tu, který je uvedený pro řídicí region. Můžete uvést různé volby chyby oblasti (REO) v nezávislé SSM oblasti a v řídicí oblasti SSM. Tabulka 66 na stránce 905 zobrazuje různé možnosti specifikací SSM.

Tabulka 66. Volby specifikace SSM

SSM pro řídicí oblast	SSM pro závislý region	Akce	Komentáře
Ne	Ne	Není	Žádný externí subsystém nemůže být připojen.
Ne	Ano	Není	Žádný externí subsystém nemůže být připojen.
Ano	Ne	Použít řídicí oblast SSM	Aplikace naplánované v oblasti mohou přistupovat k externím subsystémům označeným v řídicím regionu SSM. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do oblasti řídicí oblasti a adresních prostorů závislých oblastí.
Ano	Ano (prázdné)	Pro závislý region není použit žádný SSM.	Aplikace naplánované v této oblasti mohou přistupovat pouze k databázím DL/I. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do adresního prostoru řídicí oblasti.

Tabulka 66. Volby specifikace SSM (pokračování)			
SSM pro řídicí oblast	**SSM pro závislý region**	**Akce**	**Komentáře**
Ano	Ano (není prázdné)	Zkontrolujte SSM závislé oblasti s kontrolní oblastí SSM	Aplikace naplánované v této oblasti mohou přistupovat pouze k externím subsystémům, které jsou identifikovány v obou systémech SSM. Uživatelské procedury a řídicí bloky pro každou přílohu jsou načteny do oblasti řídicí oblasti a adresních prostorů závislých oblastí.

Neexistuje žádný specifický parametr k řízení maximálního počtu možností specifikace SSM.

Přednačítání adaptéru IMS

Výkonnost adaptéru IMS lze zlepšit, pokud je předem načtena pomocí IMS. Předložení je řízeno členem DFSMPLxx IMS.PROCLIB: viz " IMS Administration Guide: System ", kde získáte další informace. Názvy modulů IBM MQ , které mají být zadány, jsou:

CSQACLST	CSQAMLST	CSQAPRH	CSQAVICM	CSQFSALM	CSQQDEFV
PŘIPOJENÍ CSQQCONN	CSQQDISC	CSQQTERM	CSQQINIT	CSQQBACK	CSQQCMMT
CSQQESMT	PŘÍPRAVA CSQQPREP	CSQQTTHD	ČEKÁNÍ CSQQWAIT	CSQQNORM	CSQQSSOQNAME
CSQQSSSON	CSQFSTAB	CSQQRESV	CSQQSNAP	CSQQCMND	CSQCVER
CSQQTMID	CSQQTRGI	CSQQCON2	CSQBPAPI	CSQBCRMH	CSQBAPPL

Další informace o použití příkazu IBM MQ classes for JMSnaleznete v tématu Použití produktu IBM MQ classes for JMS v systému IMS.

Aktuální verze produktu IMS podporují předběžné načítání modulů IBM MQ z knihoven formátu PDS-E pouze v regionech MPP, BMP, IFP, JMP a JBP. Jakýkoli jiný typ oblasti IMS nepodporuje předběžné načítání z knihoven PDS-E. Je-li pro jakýkoli jiný typ oblasti vyžadováno předběžné načítání, musí být zadané moduly produktu IBM MQ zkopírovány do knihovny formátu PDS.

z/OS *Definování správců front IBM MQ na adaptér IMS*

Názvy správců front produktu IBM MQ a jejich odpovídající tokeny jazykového rozhraní (LITs) musí být definovány v tabulce definic správce front.

Použijte dodané makro CSQQDEFX k vytvoření zaváděcího modulu CSQQDEFV. Obrázek 117 na stránce 906 ukazuje syntaxi tohoto makra asembleru.

```
CSQQDEFX TYPE=ENTRY|DEFAULT,NAME=qmgr-name,LIT=token
or
CSQQDEFX TYPE=END
```

Obrázek 117. Syntaxe makra CSQQDEFX

Parametry

TYP=POLOŽKA|VÝCHOZÍ
Uveďte buď TYPE=ENTRY, nebo TYPE=DEFAULT takto:

TYP=POLOŽKA
Určuje, že má být vygenerována položka tabulky popisující správce front IBM MQ , který je k dispozici pro aplikaci produktu IMS . Pokud se jedná o první položku, vygeneruje se také záhlaví tabulky, včetně příkazu CSQQDEFV CSECT.

TYP=VÝCHOZÍ
Jako pro TYPE=POLOŽKA. Uvedený správce front je výchozím správcem front, který má být použit, když proměnná MQCONN nebo MQCONNX určuje název, který je prázdný. V tabulce musí být pouze jeden takový záznam.

NAME= *název-správce-front*
Uvádí název správce front, jak je uvedeno s **MQCONN** nebo **MQCONNX**.

LIT = token
Určuje název tokenu jazyka jazyka (LIT), který produkt IMS používá k identifikaci správce front.

Volání MQCONN nebo MQCONNX přidruží vstupní parametr *name* a výstupní parametr *hconn* s popiskem názvu, a tedy i LIT v položce CSQQDEFV. Další volání příkazu IBM MQ , která předává parametr *hconn* , používá LIT z položky CSQQDEFV identifikované ve volání MQCONN nebo MQCONNX k přímým voláním správce front produktu IBM MQ definovaného v rámci člena SSM produktu IMS PROCLIB se stejným LIT.

Stručně řečeno, parametr **name** na volání MQCONN nebo MQCONNX identifikuje LIT v CSQQDEFV a ve stejném LIT v členu SSM identifikuje správce front IBM MQ . (Informace o volání MQCONN naleznete v tématu MQCONN-Připojit správce front. Informace o volání MQCONNX naleznete v tématu MQCONNX-Připojit správce front (rozšířený).)

TYP=KONEC
Určuje, že tabulka je úplná. Je-li tento parametr vynechán, předpokládá se parametr TYPE=ENTRY.

Použití makra CSQQDEFX

Obrázek 118 na stránce 907 zobrazuje obecné rozvržení tabulky definic správce front.

```
CSQQDEFX NAME=subsystem1,LIT=token1
CSQQDEFX NAME=subsystem2,LIT=token2,TYPE=DEFAULT
CSQQDEFX NAME=subsystem3,LIT=token3
...
CSQQDEFX NAME=subsystemN,LIT=tokenN
CSQQDEFX TYPE=END
END
```

Obrázek 118. Rozvržení tabulky definic správce front

z/OS *Nastavení monitoru spouštěčů IMS*

Chcete-li monitorovat inicializační frontu IBM MQ , můžete nastavit dávkově orientovaný program IMS .

Definujte aplikaci pro IMS pomocí modelu CSQQTAPL v knihovně thlqual.SCSQPROC (viz Příklad definice transakce pro CSQQTRMN).

Generujte PSB a ACB za použití modelu CSQQTPSB v knihovně thlqual.SCSQPROC (viz Příklad definice PSB pro CSQQTRMN).

```
*  This is the application definition *
*  for the IMS Trigger Monitor BMP    *

APPLCTN PSB=CSQQTRMN,
PGMTYPE=BATCH,
SCHDTYP=PARALLEL
```

Obrázek 119. 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 120. Příklad definice PSB pro CSQQTRMN

Další informace o spuštění a zastavení monitoru spouštěčů IMS naleznete v tématu Ovládání monitoru spouštěčů IMS.

z/OS Nastavení mostu IMS

Most IBM MQ - IMS je volitelná komponenta, která umožňuje IBM MQ vstupu a výstupu do a z existujících programů a transakcí, které nejsou IBM MQ-enabled.

Toto téma popisuje, co je třeba udělat pro přizpůsobení mostu IBM MQ - IMS .

Definujte parametry XCF a OTMA pro IBM MQ.
Tento krok definuje názvy skupin a členů XCF pro váš systém IBM MQ a další parametry OTMA. IBM MQ a IMS musí patřit do stejné skupiny XCF. Použijte klíčové slovo OTMACON makra CSQ6SYSP , abyste přizpůsobili tyto parametry v modulu zátěže parametrů systému.

Další informace najdete v tématu Použití CSQ6SYSP .

Definujte parametry XCF a OTMA pro IMS.
Tento krok definuje názvy skupin a členů XCF pro systém IMS . IMS a IBM MQ musí patřit do stejné skupiny XCF.

Přidejte následující parametry do svého seznamu parametrů IMS , buď ve vašem JCL, nebo v členu DFSPBxxx v IMS PROCLIB:

OTMA=Y
Tím se spustí OTMA automaticky při spuštění produktu IMS . (Je volitelný, pokud zadáte OTMA=N, můžete také spustit OTMA zadáním příkazu IMS /START OTMA.)

GRNAME =
Tento parametr poskytuje název skupiny XCF.

Je to stejné jako název skupiny uvedený v definici třídy úložiště (viz další krok) a v parametru **Group** v klíčovém slově OTMACON makra CSQ6SYSP .

OTMANM =
Tento parametr udává název člena XCF systému IMS .

To je stejné jako jméno členu uvedené v definici třídy ukládání (viz další krok).

Řekněte IBM MQ skupině XCF a názvu člena systému IMS .
Toto je určeno třídou úložiště fronty. Chcete-li odesílat zprávy přes most IBM MQ - IMS , musíte je zadat při definování třídy úložiště pro frontu. Ve třídě úložiště musíte definovat skupinu XCF a název člena cílového systému IMS . Chcete-li to provést, použijte buď operace IBM MQ a ovládací panely, nebo použijte příkazy IBM MQ , jak je popsáno v části Úvod do formátu programových příkazů.

Nastavte zabezpečení, které požadujete.
Příkaz /SECURE OTMA IMS určuje úroveň zabezpečení, která má být použita pro **každý** IBM MQ správce front, který se připojuje k produktu IMS prostřednictvím modulu OTMA. Další informace najdete v tématu Aspekty zabezpečení pro použití produktu IBM MQ s produktem IMS .

Přidání dalšího připojení produktu IMS ke stejnému správci front

Chcete-li přidat připojení produktu IMS ke stejnému správci front, je třeba provést následující akce:

- Definujte druhou paměťovou třídu STGCLASS tak, aby ukazovala na nový objekt IMS; další informace viz DEFINE STGCLASS .
- Přidejte novou lokální frontu, která bude ukazovat na druhou třídu ukládání.

Důležité:

- Jedna lokální fronta nemůže ukazovat na dvě paměťové třídy.
- Jedna paměťová třída nemůže ukazovat na dva mosty IMS .
- IBM MQ a IMS musí patřit do stejné skupiny XCF. Použijte klíčové slovo OTMACON makra CSQ6SYSP , abyste přizpůsobili tyto parametry v modulu zátěže parametrů systému.

  Další informace najdete v tématu Použití CSQ6SYSP .

Související pojmy
IBM MQ a IMS
“Nastavení adaptéru IMS” na stránce 901
Použití produktu IBM MQ v rámci struktury IMS vyžaduje adaptér IBM MQ - IMS (obecně nazývaný jako adaptér IMS).

Aplikace mostu IMS a IMS v systému IBM MQ for z/OS

z/OS Použití IBM MQ s CICS

Chcete-li použít produkt IBM MQ s produktem CICS, musíte nakonfigurovat adaptér produktu IBM MQ CICS a volitelně i komponenty produktu IBM MQ CICS bridge .

Další informace o konfiguraci adaptéru IBM MQ CICS a komponent produktu IBM MQ CICS bridge naleznete v části Konfigurace připojení k produktu MQ v dokumentaci produktu CICS .

Související pojmy
IBM MQ a CICS
“Použití IBM MQ s IMS” na stránce 901
Adaptér IBM MQ -IMS a most IBM MQ - IMS jsou dvě komponenty, které umožňují produktu IBM MQ interakci s produktem IMS.

Související odkazy
“Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services” na stránce 909
Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

z/OS Upgrade a použití služby na jazykové prostředí nebo z/OS Callable Services

Akce, které musíte provést, se liší podle toho, zda používáte CALLLIBS nebo LINK, a vaši verzi SMP/E.

Následující tabulky ukazují, co je třeba provést v produktu IBM MQ for z/OS , pokud upgradujete svou úroveň nebo používáte službu na tyto produkty:

- Jazykové prostředí
- z/OS Volatelné služby (například APPC a RRS)

Tabulka 67. Služba byla použita nebo byl produkt upgradován na nové vydání

Produkt	**Akce při použití CALLLIBS a SMP/E V3r2 nebo novější** **Poznámka: Pro Jazykové prostředí a Callable Services nemusíte spouštět samostatné úlohy. Jedna práce bude stačit.**	**Akce při použití SPOJE**
Jazykové prostředí	1. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 2. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace naleznete v dokumentu *SMP/E for z/OS: Commands* . 3. Spusťte úlohu SMP/E.	Nebyla požadována žádná akce za předpokladu, že jsou zóny SMP/E nastaveny pro automatické opětovné propojení, a úloha CSQ8SLDQ byla spuštěna.
Volatelné služby	1. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 2. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace naleznete v dokumentu *SMP/E for z/OS: Commands* . 3. Spusťte úlohu SMP/E.	Nebyla požadována žádná akce za předpokladu, že jsou zóny SMP/E nastaveny pro automatické opětovné propojení, a úloha CSQ8SLDQ byla spuštěna.

Tabulka 68. Jeden z produktů byl aktualizován na nové vydání v novém prostředí SMP/E a v knihovnách

Produkt	**Akce při použití CALLLIBS a SMP/E V3r2 nebo novější** **Poznámka: Nemusíte spouštět tři samostatné úlohy pro Jazykové prostředí a Callable services. Pro oba produkty bude stačit jedna úloha.**	**Akce při použití SPOJE**
Jazykové prostředí	1. Změňte položky DDDEF pro SCEELKED a SCEESPC tak, aby ukazovala na novou knihovnu. 2. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 3. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace naleznete v dokumentu *SMP/E for z/OS: Commands* . 4. Spusťte úlohu SMP/E.	1. Odstraňte dílčí položky XZMOD pro následující položky LMOD v cílové zóně IBM MQ for z/OS : CMQXDCST, CMQXRCTL, CMQXSUPR, CSQCBE00, CSQCBE30, CSQCBP00, CSQCBP10, CSQCBR00, CSQUCVX, CSQUDLQH, CSQVXPCB, CSQVXSPT, CSQXDCST, CSQXRCTL, CSQXSUPR, CSQXTCMI, CSQXTCP, CSQXTNSV, CSQ7DRPS, IMQB23IC, IMQB23IM, IMQB23IR, IMQS23IC, IMQS23IM, IMQS23IR 2. Nastavte příslušné ZONEINDEXs mezi zónami IBM MQ a oblastmi jazykového prostředí. 3. Přizpůsobte CSQ8SLDQ tak, aby odkazovaly na novou zónu v parametru FROMZONE příkazů LINK. CSQ8SLDQ může být nalezen v knihovně SCSQINST. 4. Spusťte CSQ8SLDQ.
Volatelné služby	1. Změňte DDDEF pro CSSLIB tak, aby ukazovala na novou knihovnu 2. Nastavte hranici vaší úlohy SMP/E do cílové zóny. 3. Na kartě SMPCNTL uveďte LINK LMODS CALLLIBS. Můžete také zadat další parametry, jako je CHECK, RETRY (YES) a RC (RC). Další informace naleznete v dokumentu *SMP/E for z/OS: Commands* . 4. Spusťte úlohu SMP/E.	1. Odstraňte dílčí položky XZMOD pro následující položky LMOD v cílové zóně IBM MQ for z/OS : CMQXRCTL, CMQXSUPR, CSQBSRV, CSQILPLM, CSQXJST, CSQXRCTL, CSQXSUPR, CSQ3AMGP, CSQ3EPX, CSQ3REPL 2. Nastavte příslušnou hodnotu ZONEINDEXs mezi zónami IBM MQ a poli Volatelné služby. 3. Přizpůsobte CSQ8SLDQ tak, aby odkazovaly na novou zónu v parametru FROMZONE příkazů LINK. CSQ8SLDQ může být nalezen v knihovně SCSQINST. 4. Spusťte CSQ8SLDQ.

Příklad úlohy pro opětovné připojení modulů při použití volání CALLLIBS viz “Spuštění úlohy LINKA CALLLIBS” na stránce 911.

z/OS Spuštění úlohy LINKA CALLLIBS

Příklad úlohy pro opětovné propojení modulů při použití CALLLIBS.

Níže je uveden příklad úlohy pro opětovné propojení modulů při použití CALLLIBs na systému SMP/E V3r2 . Musíte poskytnout JOBCARD a název datové sady SMP/E CSI, které obsahuje IBM MQ for z/OS.

```
//*******************************************************************
//* RUN LINK CALLLIBS.
//*******************************************************************
//CALLLIBS EXEC PGM=GIMSMP,REGION=4096K
//SMPCSI  DD DSN=your.csi
//       DISP=SHR
//SYSPRINT DD SYSOUT=*
//SMPCNTL DD *
SET BDY(TZONE).
LINK LMODS CALLLIBS .
/*
```

Obrázek 121. 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 913

- “Uživatelská procedura rozpoznání cíle” na stránce 914

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 901

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 122 na stránce 914:

```
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 122. 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 123 na stránce 915.

```
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 123. Uživatelská procedura DRU ukázkového asembleru

V 9.1.0 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. Program Directory for IBM MQ for z/OS lze stáhnout z adresáře IBM Centrum publikací (viz IBM MQ for z/OS Program Directory PDF files).

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 917
- “Nastavení zabezpečení” na stránce 918
- “Omezení” na stránce 921

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 922
- “Automatizujte zajišťování nebo zrušení zajišťování lokálních front IBM MQ a proveďte akce pro zajištěné fronty.” na stránce 923.

Související pojmy

“nastaveníIBM MQ for z/OS” na stránce 800
Toto téma můžete použít jako vodítko pro přizpůsobení vašeho systému IBM MQ for z/OS .

V 9.1.0 z/OS Předpoklady pro z/OSMF

Nezbytné předpoklady, které potřebujete ke spuštění IBM z/OS Management Facility (z/OSMF) s IBM MQ

Sledy prací IBM MQ dodávané v produktu IBM MQ 9.1.0 využívají nové funkce v produktu z/OSMF, který je poskytován prostřednictvím oprav APAR na 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

Úloha	Popis
4	Aktualizovat tabulku vlastností programu z/OS

7. Ukázkové sledy prací a přidružené soubory jsou nainstalovány ve vhodném adresáři UNIX System Services for z/OS (USS).
8. Adresář **'/tmp'** USS 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 USS 'SLEEP' jako systémové volání.

   V závislosti na konfiguraci USS 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 ve spustitelných systémech CSQ4ZWS1.rexx a CSQ4ZWS2.rexx:

```
CALL SYSCALLS('ON')             /* Enable USS calls    */
ADDRESS SYSCALL
"SLEEP" 10                           /* Sleep for 10 seconds */
CALL SYSCALLS 'OFF'             /* Disable USS 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 916

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.

V 9.1.0 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 925.

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.

Vlastnost ID uživatele	Popis
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 .  **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 917

Nezbytné předpoklady, které potřebujete ke spuštění IBM z/OS Management Facility (z/OSMF) s IBM MQ

V 9.1.0 z/OS Omezení

Omezení při použití produktu z/OSMF s produktem IBM MQ.

1. Sled prací produktu `provision.xml` v současné době automatizuje následující zvýrazněné úlohy přizpůsobení správce front:

Úloha	Popis
1	Identifikace systémových parametrů produktu z/OS .
2	Autorizace APF autorizuje zaváděcí knihovny IBM MQ **(provision.xml provádí APF autorizovat některé knihovny)**
3	Aktualizovat seznam odkazů z/OS a LPA
4	Aktualizace tabulky vlastností programu z/OS
5	**Definujte subsystém IBM MQ k produktu z/OS**
6	**Vytvoření procedur pro správce front produktu IBM MQ**
7	**Vytvořit procedury pro inicializátor kanálu**
8	**Definice subsystému IBM MQ pro třídu služeb z/OS WLM**
9	Vyberte a nastavte prostředí úložiště odlehčování pro prostředek Coupling Facility.
10	Nastavení prostředku CF
11	Provádět ovládací prvky zabezpečení ESM
12	Aktualizujte SYS1.PARMLIB členové
13	**Upravit vstupní datové sady inicializace**
14	**Vytvoření zaváděcího programu a datových sad protokolu**
15	**Definujte sady stránek**
16	Přidejte položky produktu IBM MQ do skupiny sdílení dat produktu Db2 .
17	**Přizpůsobte moduly parametrů systému (některé)**
18	**Přizpůsobte parametry inicializátoru kanálu (některé)**
19	Nastavení adaptérů dávek, TSO a RRS
20	Nastavení operací a ovládacích panelů
21	Zahrnout člena formátování výpisu paměti IBM MQ
22	Potlačit informační zprávy
23	Aktualizujte vašeho systémového člena DIAG pro Advanced Message Security
24	Vytvořit procedury pro Advanced Message Security
25	Nastavení spuštěné úlohy rozšířené zprávy uživatele spuštěné úlohy
26	Udělte oprávnění RACDCCERT administrátorovi zabezpečení pro produkt Advanced Message Security

Úloha	Popis
27	Udělte uživatelům oprávnění k prostředkům pro produkt Advanced Message Security

2. Úlohy přizpůsobení, které nejsou zvýrazněny tučným písmem, musí být provedeny ručně, je-li to nutné.
3. Ukázkové členy INP1 a INP2 jsou v současné době používány stejně jako. Je-li to nutné, mohou být definovány další vlastnosti pro řízení prostředků definovaných těmito členy.
4. Komentáře týkající se specifických vlastností uvedených v souboru vlastností indikují veškerá omezení použití těchto vlastností. Další informace naleznete v tématu “Spuštění sledů prací” na stránce 925.

Související pojmy

“Nastavení zabezpečení” na stránce 918
Nastavení zabezpečení požadovaná ke spuštění produktu z/OSMF.

V 9.1.0 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 925. **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).

Název sledu prací	Popis
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 925.

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

Název sledu prací	Popis
	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 925.
offloadQueue.xml	Odlehčení zpráv z lokální fronty do datové sady. 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 925.
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 925.

Související pojmy

“Omezení” na stránce 921
Omezení při použití produktu z/OSMF s produktem IBM MQ.

V 9.1.0 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

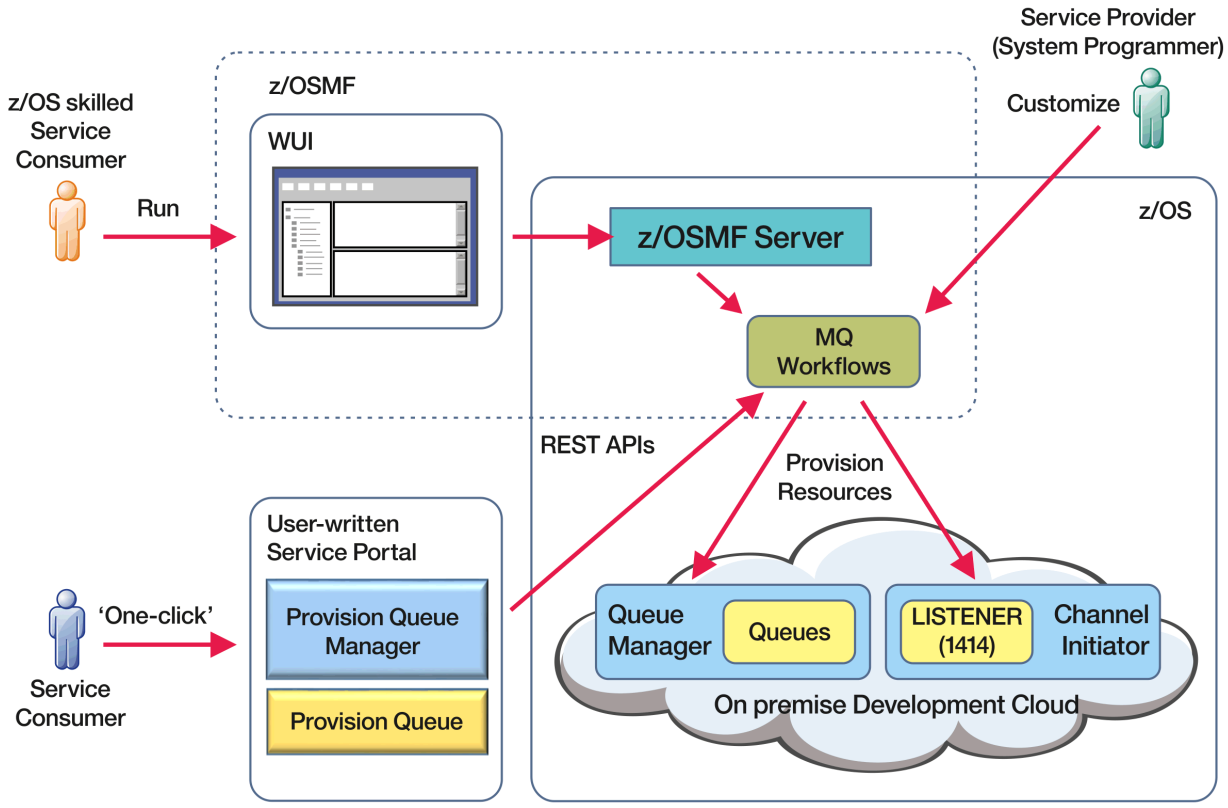
Následující soubory deklarují proměnné, na které odkazují ukázkové sledy prací z/OSMF a přidružené soubory JCL nebo REXX exec:

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 124. 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 922

Ukázky jsou dodávány pro automatizaci zajišťování správců front a lokálních front.

V 9.1.0 z/OS MQ Adv. VUE Konfigurace produktu IBM MQ Advanced for z/OS VUE

Pomocí těchto informací můžete konfigurovat funkce, které jsou k dispozici s nárokem produktu IBM MQ Advanced for z/OS VUE .

Informace o této úloze

Můžete povolit vzdálená připojení agenta Managed File Transfer s produktem IBM MQ Advanced for z/OS Value Unit Edition.

Můžete využít možnosti připojení ze správců front produktu IBM MQ Advanced for z/OS Value Unit Edition ke službě IBM Blockchainv produktu IBM Cloud (formerly Bluemix).

V 9.1.0 Můžete připojit IBM MQ classes for JMSnebo IBM MQ classes for Java, aplikaci ke správci front v systému z/OS, který má atribut **ADVCAP(ENABLED)** , a to pomocí připojení klienta. Další informace naleznete v tématu Konektivita klientaJava a JMS pro správce front z/OS.

Postup

1. Povolte vzdálená připojení agenta Managed File Transfer s produktem IBM MQ Advanced for z/OS Value Unit Edition.
2. Nakonfigurujte produkt IBM MQ Advanced for z/OS VUE pro použití se službou IBM Blockchain v produktu IBM Cloud.

V 9.1.0 z/OS MQ Adv. VUE Povolení konektivity agenta MFT ke vzdáleným správcům front produktu z/OS

Agenti Managed File Transfer na systému z/OS, kteří jsou spuštění pod identifikátorem produktu (PID) produktu IBM MQ Advanced for z/OS VUE, se mohou připojit ke vzdálenému správci front v produktu z/OS pomocí připojení klienta.

Když se agent spustí, zapíše zprávu BFGPR0137I do svého protokolu událostí (output0.log) zobrazující PID, pod kterým je spuštěn. Příklad této zprávy je:

```
BFGPR0137I: Byl zahájen záznam dat použití produktu pro produkt 'MQ z/OS MFT', ID produktu '5655-MF9'.
```

Podrobnosti o produktech IBM MQ , jejich přidružených hodnotách PID a exportních klasifikacích najdete v tématu Identifikátory produktuIBM MQ a informace o exportu.

Agent MFT na systému z/OSspuštěný pod libovolným identifikátorem PID se může připojit k lokálnímu správci front pouze pomocí připojení vazeb.

Agent produktu MFT v produktu z/OS se může připojit pouze ke správci front, který je rovněž spuštěn v produktu z/OS, bez ohledu na identifikátor PID produktu MFT .

Pokud se agent IBM MQ Advanced for z/OS VUE pokusí o připojení ke správci front, který není spuštěn v systému z/OS, zobrazí se zpráva BFGQM1044E: `Připojení klienta agenta v systému z/OS musí být pro správce front v systému z/OS` a spuštění agenta se ukončí.

Související úlohy

Spuštění agenta MFT na systému z/OS

V 9.1.0 z/OS Linux MQ Adv. VUE

Konfigurace produktu IBM MQ Advanced for z/OS VUE pro použití s blockchain

Nastavte a spusťte program IBM MQ Bridge to blockchain pro bezpečné připojení IBM MQ ve správci front z/OS a IBM Blockchain. Pomocí mostu pro asynchronní připojení se můžete vyhledat a aktualizovat stav prostředku ve vašem řetězci blockchain pomocí aplikace systému zpráv, která se připojuje ke správci front produktu IBM MQ Advanced for z/OS VUE .

Než začnete

- Produkt IBM MQ Bridge to blockchain je k dispozici jako součást sady Connector Pack v produktu IBM MQ Advanced for z/OS Value Unit Edition 9.1.0. Můžete se připojit ke správcům front produktu IBM MQ Advanced for z/OS VUE , kteří jsou spuštění na stejné úrovni příkazů, nebo výše.
- IBM MQ Bridge to blockchain je podporováno pro použití se svou sítí blockchain, která je založena na Hyperledger Composer postavených na Hyperledger Fabric.
- Produkt IBM MQ Bridge to blockchain musí být nainstalován v prostředí služeb systému UNIX a vyžaduje Java runtime environment 8 z produktu IBM.

Informace o této úloze

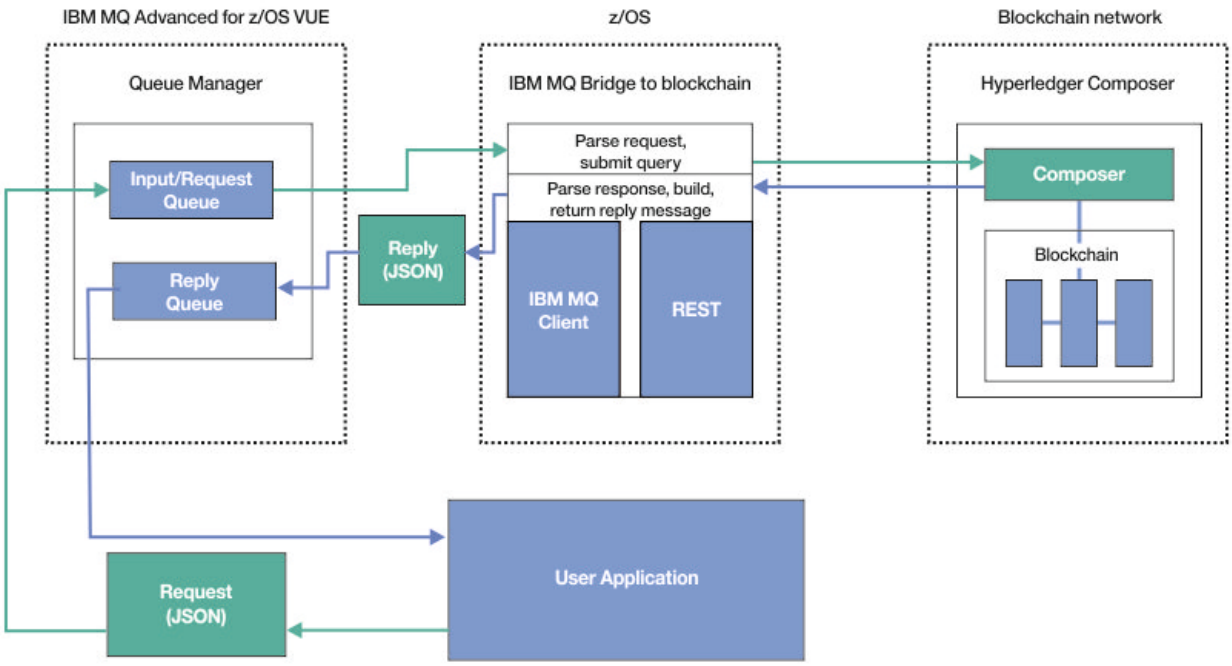
Blockchain je sdílená, distribuovaná digitální kniha, která se skládá z řetězce bloků, které představují odsouhlasené transakce mezi objekty typu peer v síti. Každý blok v řetězci je propojen s předchozím blokem atd. zpět k první transakci.

Produkt IBM Blockchain je postaven na systémech Hyperledger Fabric a Hyperledger Composer. Můžete se s ním vyvíjet lokálně pomocí produktu Dockernebo v kontejneru kontejneru v produktu IBM Cloud. Můžete také aktivovat a používat svou síť IBM Blockchain ve výrobě, vytvářet a spravovat obchodní síť s vysokou úrovní zabezpečení, soukromí a výkonu. Další informace naleznete v příručce IBM Blockchain Platform.

Hyperledger Fabric a Hyperledger Composer jsou open source, podnikový blockchain framework, který je vyvíjen ve spolupráci s členy Hyperledger Project, včetně IBM jako výchozího přispěvatele kódu. Hyperledger Project, nebo Hyperledgerje Linux Foundation open source, global, collaborative initiative to advance cross-industry blockchain technologies. Další informace viz IBM Blockchain, ProjektyHyperledger, Hyperledger Fabrica Hyperledger Composer.

Pokud již používáte produkt IBM MQ Advanced for z/OS VUE a IBM Blockchain, můžete použít produkt IBM MQ Bridge to blockchain k řízení svého obchodního modelu produktu Hyperledger Composer prostřednictvím rozhraní REST produktu Hyperledger Composer , což vám umožní aktualizovat nebo dotazovat se na stav blockchain a přijímat odpovědi zpět ze sítě blockchain. Tímto způsobem můžete integrovat místní software produktu IBM se službou blockchain cloudu nebo lokálně provozovaným řešením.

Stručný přehled operačního procesu mostu lze zobrazit na obrázku 1. Uživatelská aplikace vloží ve správci front z/OS ve vstupní/výstupní frontě zprávu naformátovanou ve formátu JSON. Při použití serveru REST produktu Hyperledger Composer se most připojuje ke správci front, získává zprávu ze vstupní/fronty požadavků, zkontroluje, zda je JSON správně naformátovaný, a pak vydá požadavek REST do bloku blockchain. Data vrácená blockchasem je analyzována mostem a umístěna do fronty odpovědí, jak je definováno v původní zprávě požadavku IBM MQ . Uživatelská aplikace se může připojit ke správci front, získat zprávu odpovědi z fronty odpovědí a použít tyto informace.



Obrázek 125. IBM MQ Bridge to blockchain

Server IBM MQ Bridge to blockchain je třeba nakonfigurovat tak, aby se připojoval k serveru Hyperledger Composer REST, a nikoli přímo k základní vrstvě produktu Hyperledger Fabric . Je-li spuštěn most, aplikace systému zpráv požaduje, aby most řídil rozhraní REST API produktu Hyperledger Composer na základě uživatelsky definovaného modelu obchodní sítě, který dále řídí podkladové rutiny řetězového kódu, které mohou dotazovat nebo aktualizovat stav prostředku, a vrátit výsledky jako odezvu pomocí serveru Hyperledger Composer REST, do aplikace systému zpráv.

Postup

Vytvořte fronty pro most tak, že upravíte a odešlete ukázku JCL v produktu `thlqual.SCSQPROC(CSQ4BCBQ)`.

Pro výchozí pojmenované fronty, které se používají pro následující fronty, jsou k dispozici ukázkové definice front mostu:

- Vstup zprávy na most: `SYSTEM.BLOCKCHAIN.INPUT.QUEUE`a `APPL1.BLOCKCHAIN.INPUT.QUEUE`
- Odpovědi z řetězce blockchain: `APPL1.BLOCKCHAIN.REPLY.QUEUE`

Různé aplikace mohou používat stejnou vstupní frontu, ale můžete uvést více front odpovědí, jednu pro každou z vašich aplikací. Není nutné používat definované fronty odpovědí. Chcete-li používat dynamické fronty pro odpovědi, musíte zvážit jejich konfiguraci zabezpečení.

Výsledky

Vytvořili jste fronty, které most vyžaduje ke zpracování zpráv z produktu IBM MQ a ze sítě blockchain.

Jak pokračovat dále

Použijte informace o správci front a pověření ze sítě blockchain k vytvoření konfiguračního souboru pro produkt IBM MQ Bridge to blockchain.

V 9.1.0 z/OS MQ Adv. VUE Vytvoření konfiguračního souboru pro IBM MQ Bridge to blockchain

Zadejte správce front a parametry sítě blockchain, chcete-li vytvořit konfigurační soubor pro produkt IBM MQ Bridge to blockchain pro připojení k sítím IBM MQ a IBM Blockchain .

Než začnete

- Vytvořili jste a nakonfigurovali síť blockchain Hyperledger Composer .
- Nainstalovali jste produkt IBM MQ Bridge to blockchain ve svém prostředí z/OS .
- Byl spuštěn správce front produktu IBM MQ Advanced for z/OS VUE .

Informace o této úloze

Tato úloha vás provede minimálním nastavením potřebným k vytvoření konfiguračního souboru produktu IBM MQ Bridge to blockchain a k úspěšnému připojení k sítím IBM Blockchain a IBM MQ .

Most je možné použít k připojení k sítím blockchain, které jsou založeny na produktu Hyperledger Composer. Chcete-li použít most, potřebujete informace o konfiguraci ze sítě blockchain. V každém kroku v této úloze můžete najít příklad podrobností konfigurace, které jsou založeny na dvou různých konfigurovaných sítích blockchain:

- Hyperledger Composer sítě, která běží v produktu Docker. Další informace viz téma Instalace produktu Hyperledger Composera Generování rozhraní API služby REST.
- Síť Hyperledger Composer , která se spouští v klastru Kubernetes v produktu IBM Cloud. Další informace viz Vývoj v pískovišti cloudu na platformě IBM Blockchain Platform.

Další informace o významu a volbách pro všechny parametry obslužného programu IBM MQ Bridge to blockchain naleznete v popisu příkazu runmqbcb . Musíte zvážit své vlastní požadavky na zabezpečení a přizpůsobit parametry vhodné pro vaši implementaci.

Postup

1. Chcete-li vytvořit konfigurační soubor, spusťte most v prostředí systémového shellu systému UNIX (USS).

   Parametry potřebujete z informací o zabezpečení produktu Hyperledger Composer a z vašeho správce front produktu IBM MQ Advanced for z/OS VUE .

   Spusťte skript mostu z adresáře `mqbc/bin` v umístění USS, kde je nainstalován produkt IBM MQ .

   ```
   ./runmqbcb -o config_file_name.cfg
   ```

   Jak ukazuje následující příklad, existující hodnoty jsou zobrazeny v hranatých závorkách. Stiskněte tlačítko `Enter` , chcete-li přijmout existující hodnoty, stiskněte `Space` a pak `Enter` , abyste vymazali hodnoty, a zapište do hranatých závorek a pak stiskněte klávesu `Enter` pro přidání nových hodnot. Můžete oddělit seznamy hodnot (např. rovnocenných uzlů) čárkami nebo každou hodnotu na novém řádku. Prázdný řádek ukončí seznam.

   Poznámka: Existující hodnoty nelze upravovat. Můžete je zachovat, nahradit nebo vymazat.
2. Zadejte hodnoty pro připojení ke správci front produktu IBM MQ Advanced for z/OS VUE .

   Minimální hodnoty, které jsou potřeba pro připojení, jsou název správce front a názvy vstupních front mostu, které jste nadefinovali. Pro připojení ke vzdáleným správcům front IBM MQ Advanced for z/OS VUE je třeba také **`MQ Channel`** a **`MQ Conname`** (hostitelská adresa a port, kde je správce front spuštěn).

   Chcete-li používat TLS pro připojení k produktu IBM MQ v kroku “5” na stránce 931, musíte použít rozhraní JNDI nebo tabulky CCDT a v souladu s tím uvést **`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 vaší síti blockchain (je-li konfigurována).

   V následujícím příkladu byl server Hyperledger Composer REST nakonfigurován pomocí úložiště pověření LDAP pomocí modulu **passport-ldapauth NodeJS** . Všimněte si, že tímto způsobem lze použít kterýkoli z modulů produktu **passport-*** , který poskytuje základní pověření 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, který je `http` nebo `https`, a že číslo portu je povinné. Zda je použit protokol HTTP nebo HTTPS, závisí na konfiguraci zabezpečení serveru REST. Pokud je na server REST poskytnuta dvojice certifikátu a soukromého klíče, použije se HTTPS. Je použit protokol HTTPS. Jinak se použije HTTP. Další informace o tom, jak určit dvojici certifikátu a soukromého klíče, naleznete v kroku “5” na stránce 931.

```
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 IBM MQ JMS , který se připojuje ke správci front, což znamená, že může být konfigurován tak, aby používal zabezpečení TLS k bezpečnému připojení se stejným způsobem jako jakýkoli jiný klient produktu IBM MQ JMS . Konfigurace podrobností o připojení TLS je vystavena pouze poté, co uvedete informace JNDI nebo CCDT v kroku “2” na stránce 930.

   Úložiště certifikátů se používají pro produkt Hyperledger Composera pro správce front produktu IBM MQ Advanced for z/OS VUE . Jsou-li určena úložiště certifikátů, most se vždy pokusí připojit k serveru REST produktu Hyperledger pomocí protokolu HTTPS. TLS však lze pro IBM MQ zakázat, ale stále používá TLS pro Hyperledger Composer pomocí 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 téma Zabezpečení serveru REST pomocí HTTPS a TLS.

6. Volitelné: Zadejte umístění souboru protokolu pro IBM MQ Bridge to blockchain.

   V konfiguračním souboru nebo na příkazovém řádku můžete zadat název a umístění souboru protokolu.

```
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

Postupujte podle kroků pro “Spuštění prostředí IBM MQ Bridge to blockchain” na stránce 933

Související odkazy

runmqbcb (spuštění příkazu IBM MQ Bridge to blockchain)

V 9.1.0 z/OS Konfigurace zabezpečení produktu IBM MQ pro produkt IBM MQ Bridge to blockchain

Pokyny pro nastavení zabezpečení produktu IBM MQpomocí produktu IBM MQ Bridge to blockchain.

Následující příklady zobrazují definice RACF, které lze použít k poskytnutí přístupu produktu IBM MQ Bridge to blockchain k frontám, které potřebuje. Definice předpokládají, že most je spuštěn pod ID uživatele MQBCBUSR.

Kromě toho je třeba, aby byl produkt IBM MQ Bridge to blockchain udělen přístup pro připojení ke správci front, a to buď:

- Přímo s použitím režimu vázání; viz Profily zabezpečení připojení pro dávkové připojenínebo
- Použití režimu klienta prostřednictvím kanálu CHINIT; viz Požadavky klienta MQI

Autorizace pro frontu požadavků IBM MQ Bridge to blockchain

Zadáním následujících příkazů RACF udělte uživateli MQBCBUSR přístup pro příjem zpráv z výchozího nastavení SYSTEM.BLOCKCHAIN.INPUT.QUEUE fronta požadavků:

```
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 uživateli MQBCBUSR přístup ID uživatele k odeslání zpráv do souboru APPL1.BLOCKCHAIN.REPLY.QUEUE. Tento název fronty je zadán v odpovědi na název fronty ve zprávě s požadavkem:

```
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” na stránce 792

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

Rozhraní API-rychlý odkaz na zabezpečení přístupu k prostředkům

V 9.1.0 z/OS MQ Adv. VUE 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 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 produktu UNIX System Services (USS) z adresáře `mqbc/bin` v umístění USS, 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 ++PATHPREFIX++ instalační cestou IBM MQ for z/OS USS Components.
   - Nahraďte proměnnou ++CONFIGFILE++ cestou ke konfiguračnímu souboru vytvořenému pomocí příkazu `runmqbc -o <file>` z USS.
   - 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” na stránce 792 .
- 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.

V 9.1.0 z/OS *Formáty zpráv pro IBM MQ Bridge to blockchain před IBM MQ 9.1.4*

Informace o formátování zpráv, které jsou odesílány a přijímány produktem IBM MQ Bridge to blockchain.

LTS

Upozornění: Existující formát pro formáty zpráv je zastaralý. From IBM MQ 9.1.4, if you have a Hyperledger Fabric network, use the format of the messages described in “Formáty zpráv pro IBM MQ Bridge to blockchain z IBM MQ 9.1.4” na stránce 790.

Aplikace požaduje, aby IBM MQ Bridge to blockchain řídil Hyperledger Composer definované rozhraní API REST tak, aby postupovali na informace, které jsou drženy na řetězci blockchain. Aplikace to provede umístěním zprávy s požadavkem do fronty požadavků mostu. Výsledky požadavku REST jsou formátovány podle mostu 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 požadavku obsahují tři atributy:

metoda
Příkazové slovo REST použité pro volání rozhraní REST API produktu Hyperledger Composer , jako např. POST, DELETE nebo GET

path
Cesta k rozhraní REST API produktu Hyperledger Composer . Tato hodnota je přidána k základní adrese URL serveru. Cesta by měla začínat řetězcem `"api/"`.

tělo
Obsah specifický pro danou metodu. To je často struktura JSON.

Následující příklad používá metodu POST k cestě `api/Traderk` vytvoření nového objektu Truder. Tělo uvádí třídu Traders, jak je definováno modelem Hyperledger Composer uživatele, a také uvádí další hodnoty potřebné k vytvoření nového Obchodního objektu v síti blockchain.

```
{ "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 nastavené na ID zprávy příchozí zprávy. Libovolné uživatelem definované vlastnosti se zkopírují ze zprávy požadavku do zprávy odpovědi. ID uživatele v odpovědi je nastaveno na ID uživatele původce.

statusCode je stavový kód HTTP. Je-li chyba z IBM MQ nebo z mostu, pak se použije odpovídající **statusCode** .

statusType je řetězec, buď *SUCCESS* , nebo *FAILURE*.

Pro úspěšné požadavky obsahuje prvek "**data**" ve zprávě odpovědi odpověď z vyvolaného rozhraní REST API produktu Hyperledger Composer .

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 odezvy na chybu 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 selhal při zpracování serverem REST produktu Hyperledger Composer

```
{
   "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, a to buď při pohledu na řetězec **statusType** , nebo z existence datového pole. Pokud při zpracování vstupní zprávy došlo k chybě a most jej neodesílá do bloku blockchain, je hodnota vrácená z mostu hodnotou MQRC, obvykle **MQRC_FORMAT_ERROR**.

V 9.1.0 z/OS *Spuštění ukázky klienta IBM MQ Bridge to blockchain*

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 k vašemu IBM MQ Advancednebo IBM MQ Advanced for z/OS VUE, správci front a 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 USS, kde jsou nainstalovány komponenty USS 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 "0K" 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.

Konfigurace produktu IBM MQ Internet Pass-Thru

Tato sekce popisuje různé funkce, které IBM MQ Internet Pass-Thru (MQIPT) podporuje a jak je nakonfigurovat.

Vlastnosti, které lze zadat v konfiguračním souboru MQIPT , jsou popsány v Referenční příručce konfigurace produktuIBM MQ Internet Pass-Thru.

Podpora HTTP v produktu MQIPT

Produkt MQIPT podporuje tunelové připojení HTTP. Produkt MQIPT lze nakonfigurovat tak, aby datové pakety, které jsou předávány, byly kódovány jako požadavky HTTP.

Kanály IBM MQ nepřijímají požadavky HTTP. Proto je pro příjem požadavků HTTP a jejich převedení zpět do normálních paketů protokolu IBM MQ je nutný druhý příkaz MQIPT . Druhý příkaz MQIPT odstraní záhlaví HTTP, aby převedl příchozí paket zpět na standardní paket protokolu IBM MQ před předáním do cílového správce front.

Když se používá HTTP mezi dvěma instancemi produktu MQIPT, připojení TCP/IP, na kterém je tok požadavků a odpovědí HTTP je trvalý a je ponechán otevřený po celou dobu životnosti kanálu zpráv. Produkt MQIPT nezavře spojení TCP/IP mezi dvojicemi požadavek/odpověď.

Pokud dvě instance produktu MQIPT komunikují prostřednictvím protokolu HTTP, je možné, že by požadavek HTTP mohl zůstat nevyrovnaný po delší dobu. Příklad je v kanálu žadatele/serveru, kdy strana serveru čeká na příchod nových zpráv do přenosové fronty. Poskytují se protokol kanálu produktu IBM MQmechanismus "heartbeat", který vyžaduje pravidelné čekání na odeslání synchronizačních zpráv svému partnerovi. Výchozí perioda prezenčního signálu kanálu je 5 minut. MQIPT používá tento prezenční signál jako odpověď HTTP. Nezakazujte tento prezenční signál kanálu nebo jej nastavte na příliš vysokou hodnotu, abyste se vyhnuli problémům s vypršením časového limitu v některých bránách firewall.

Produkt MQIPT přijímá přenos HTTP ve formátu chunked, který je generován serverem proxy nebo serverem HTTP.

Příklad použití protokolu HTTP v produktu MQIPTnajdete v tématu Konfigurace tunelového propojení HTTP.

servery proxy HTTP

Server proxy HTTP může být umístěn mezi dvě instance produktu MQIPT. Server proxy HTTP musí splňovat následující požadavky:

- Server proxy musí podporovat protokol HTTP 1.1 .
- Hlavičky HTTP **Connection** nebo **Proxy-Connection** , které jsou nastaveny produktem MQIPT , musí být uznány serverem proxy. To umožňuje ponechat spojení mezi dvěma instancemi portálu MQIPT po celou dobu životnosti kanálu zpráv.
- V rámci serveru proxy musí být udržováno mapování trvalých spojení jeden na jeden. Tím je zajištěno, že připojení TCP/IP ze serveru proxy do místa určení MQIPT nebudou použita k přenosu dat pro více než jeden kanál zpráv.

Můžete nastavit vlastnosti konfigurace způsobu, jakým jsou trvalá připojení spravována na některých serverech proxy HTTP. Například můžete být schopni nastavit maximální počet požadavků, které lze provést u trvalého připojení. Měly by být nastaveny následující vlastnosti:

- Trvalá připojení by měla být povolena.
- Opětovné použití připojení TCP/IP ze serveru proxy do produktu MQIPT by mělo být zakázáno více než jednou relací HTTP, aby se zachovalo mapování trvalých spojení přes proxy na jeden-jeden-jeden.
- Časový limit pro požadavky proxy by měl být nastaven na vysokou hodnotu. Například 12 hodin.
- Maximální počet požadavků, které lze provést v trvalém připojení, by měl být nastaven na vysokou hodnotu. Například 5000.

Produkt MQIPT používá požadavky HTTP **POST** k odesílání dat mezi dvěma instancemi produktu MQIPT. Pokud konfigurace produktu MQIPT určuje název hostitele serveru proxy pomocí vlastnosti **HTTPProxy** , MQIPT se připojí k serveru proxy a použije metodu HTTP **CONNECT** k požadavku, aby server proxy vytvořil tunel do místa určení MQIPT. To umožňuje průchod HTTPS přes proxy, aniž by se ukončila relace TLS na serveru proxy.

Je-li mezi instancemi produktu MQIPT umístěn prostředek pro rozložení zátěže, musí být nakonfigurován tak, aby používal hodnotu souboru cookie HTTP *MQIPTSessionId* , aby bylo zajištěno, že všechny požadavky na každou relaci budou předány do stejného cíle.

HTTPS v produktu MQIPT

Protokol HTTPS lze použít na připojení HTTP tak, že povolíte vlastnosti směrování **HTTPS** a **SSLClient** na serveru MQIPT , který vydává připojení klienta.

Produkt MQIPT musí mít přístup k důvěryhodnému certifikátu CA, který se použije k ověření cíle HTTP proxy/serveru. Vlastnost **SSLClientCAKeyring** lze použít k definování souboru svazku klíčů obsahujícího důvěryhodný certifikát CA.

Obecné nastavení pro HTTPS bude používat lokální server proxy HTTP pro tunel ven přes bránu firewall a připojit se ke vzdálenému serveru HTTP (nebo jinému serveru proxy), který se zase připojí ke vzdálenému serveru MQIPT. Tento MQIPT na straně serveru připojení nevyžaduje žádnou specifickou konfiguraci, protože požadavek na připojení je považován za normální připojení HTTP.

MQIPT používá vlastnosti **HTTPProxy** a **HTTPServer** k rozlišení lokálních a vzdálených serverů proxy. Trasa MQIPT s nastavenou vlastností **HTTPProxy** je považována za lokální server proxy HTTP a cesta MQIPT se sadou vlastností **HTTPServer** je vzdálený server (nebo server proxy).

Připojení HTTPS se obvykle provádí na adresu portu modulu listener 443 na serveru HTTP proxy/server, ale vlastnosti **HTTPProxyPort** a **HTTPServerPort** lze použít k přepsání této předvolby.

Podpora SOCKS v MQIPT

Server proxy SOCKS je síťová služba používaná jako řízený bod předání prostřednictvím brány firewall. Aplikace SOCKS zapnuta, spuštěná uvnitř ochranné bariéry, může použít proxy SOCKS pro připojení ke vzdálené aplikaci.

Produkt MQIPT se může chovat jako proxy SOCKS povolením vlastnosti **SocksServer** , čímž umožňuje aplikacím IBM MQ s povoleným SOCKS připojit se přes MQIPT ke vzdálenému správci front IBM MQ . Při použití této funkce se cílová cílová adresa a adresa cílového portu získávají během procesu navázání komunikace přes 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 fungovat jako klient SOCKS, a to v zastoupení lokální aplikace IBM MQ , která nebyla povolena SOCKS. To je užitečné při používání brány firewall, která povoluje odchozí připojení pouze přes server proxy SOCKS. Každou přenosovou cestu MQIPT lze nakonfigurovat tak, aby komunikovala s jiným proxy SOCKS.

Příklad použití SOCKS najdete v tématu Konfigurace serveru proxy SOCKS .

klastrování v produktu MQIPT

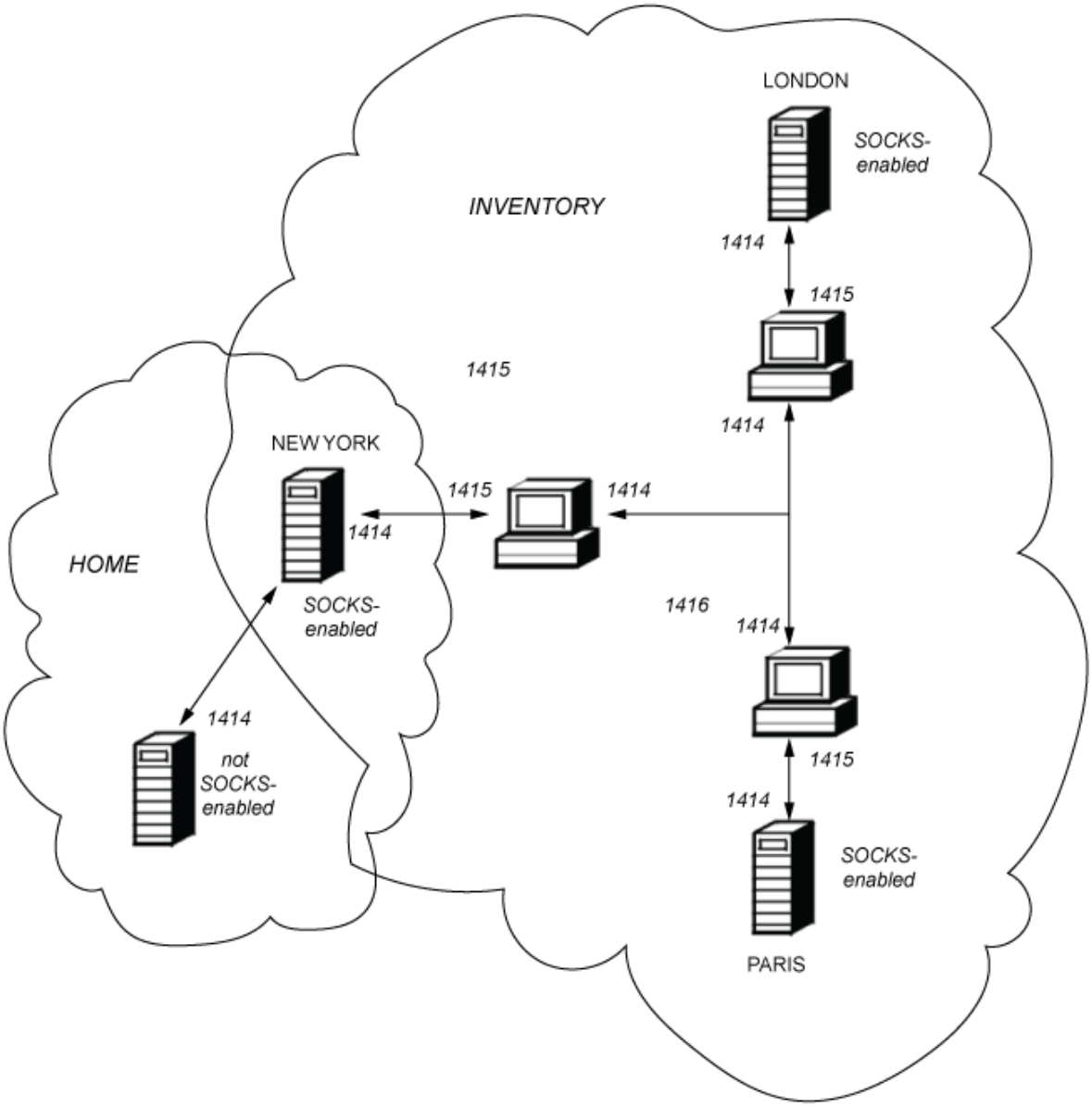
Klastry IBM MQ lze použít s produktem MQIPT prostřednictvím protokolu SOCKS-povolení každého správce front v klastru, který je umístěn v síti Internet, a povolením produktu MQIPT fungovat jako server proxy SOCKS.

V následujícím diagramu jsou NEWYORK a CHICAGO nacházejí v klastru nazvaném HOME a v obou úložištích se nacházejí úplná úložiště. NEWYORK, LONDÝN a PARIS jsou v jiném klastru nazvaném INVENTORY. Všimněte si, že CHICAGO nemusí být SOCKS, protože se nachází v klastru, který nepotřebuje MQIPT.

Každý správce front v klastru INVENTORY je efektivně "skrytý" za MQIPT. Vzhledem k tomu, že správce front byl při spuštění kanálu odesílatele klastru povolen protokol SOCKS, odešle se požadavek do místa určení pomocí serveru MQIPT , který se chová jako server proxy SOCKS. Za normálních okolností se položka CONNAME v kanálu příjemce klastru používá k identifikaci lokálního správce front, ale při použití s produktem MQIPTmusí CONNAME identifikovat lokální MQIPT a jeho příchozí port modulu listener. V následujícím diagramu jsou všechny příchozí adresy portů modulu listener 1414 a adresy portu odchozího modulu listener jsou 1415.

Existují dva způsoby, jak spustit správce front s podporou SOCKS. První z nich je SOCKS-povolte celý počítač, kde je spuštěn správce front. Druhá hodnota je SOCKS-povolit pouze správce front. Při použití obou metod je nutné konfigurovat klienta SOCKS, aby bylo možné používat pouze vzdálená připojení pomocí produktu MQIPT jako serveru proxy SOCKS a zakázat ověřování uživatelů. Pro podporu SOCKS je na trhu mnoho produktů. Musíte zvolit takový, který podporuje protokol SOCKS V5 .

Příklad, jak nakonfigurovat klastrovou síť, najdete v tématu Konfigurace podpory klastrování produktu MQIPT .



Podpora SSL/TLS v MQIPT

Zabezpečené sokety lze použít k zajištění soukromí komunikace, integrity komunikace a ověření.

Ochrana soukromí komunikace
Spojení může být vytvořeno jako soukromé. Data, která se mají vyměňovat mezi klientem a serverem, mohou být šifrována a pouze odesilatel a příjemce může dávat smysl pro data. To znamená, že soukromé informace, jako např. čísla kreditních karet, mohou být přenášeny bezpečně.

Integrita komunikace
Spojení je spolehlivé. Přenos zprávy zahrnuje kontrolu integrity zpráv založenou na zabezpečené transformační funkci.

Ověřování
Klient může ověřit identitu klienta a autentizovaný 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 (certifikátůX.509v3).

Protokoly zabezpečeného soketu

V produktu MQIPTjsou zabezpečené sokety poskytovány pomocí protokolů TLS (Transport Layer Security) a SSL (Secure Sockets Layer). Tyto dva protokoly zabezpečeného soketu jsou podobné, ale nespolupracují. V této dokumentaci jsou výrazy SSL a TLS používány zaměnitelně, pokud není zaznamenán specifický rozdíl.

Produkt MQIPT podporuje zabezpečení SSL 3.0, TLS 1.0, TLS 1.1a TLS 1.2 poskytované dodávaným produktem Java runtime environment (JRE). IBM MQ CipherSpec vzdáleného kanálu určuje, který protokol MQIPT používá.

SSL 3.0 je nezabezpečeno a je v produktu MQIPTstandardně vypnuto. V 9.1.4 TLS 1.0 a TLS 1.1 jsou také standardně zablokovány v produktu MQIPT z IBM MQ 9.1.4. Potřebujete-li použít některý z těchto zakázaných protokolů, lze je znovu povolit pomocí postupu uvedeného v části “Povolení zamítnutých protokolů a CipherSuites v produktu MQIPT” na stránce 964.

Protokoly SSL/TLS mohou používat různé algoritmy digitálních podpisů pro ověřování komunikačních stran. Operace šifrování, které se používají v SSL/TLS, šifrování pro utajení dat a zabezpečené hašování pro integritu zpráv, se 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.

Šifrovací komponenta prostředí JRE

Šifrovací komponenta SSL/TLS pro prostředí JRE obsahuje poskytovatele zabezpečení IBMJSSEFIPS a IBMJCEFIPS, kteří jsou certifikováni kompatibilní s FIPS 140-2 na úrovni 1. Tito poskytovatelé zabezpečení mají v prostředí JRE nejvyšší prioritu, takže jsou implementace s certifikací FIPS používány všude tam, kde jsou k dispozici. Podporovány jsou různé kryptografické algoritmy. Určete je pomocí protokolu SSL/TLS CipherSuites. Ne všechny CipherSuites jsou certifikovány FIPS 140-2.

Režim přemostění SSL/

Je-li přenosová cesta nastavena na hodnotu SSLServer i SSLClient, přijímá MQIPT jedno příchozí připojení SSL/TLS a zavádí druhé zabezpečené připojení SSL/TLS k jinému MQIPT nebo cílovému správci front. Informace o kanálu produktu IBM MQ jsou mezi těmito dvěma připojeními SSL/TLS dešifrovány a znovu šifrovány. Jako přemostění SSL/TLS se také odkazuje jako na *server proxy ukončení SSL/TLS*.

Produkt IBM MQ podporuje přemostění SSL/TLS pomocí produktu MQIPT. Bylo zjištěno, že další servery proxy pro ukončení SSL/TLS s IBM MQ mohou způsobit nefunkční připojení, pokud server proxy kombinuje nebo rekonstruuje záznamy SSL/TLS s různými velikostmi, než které byly odeslány příkazem IBM MQ. Důvodem je interakce mezi správci fronty přidělovat a spravovat paměť pro příchozí data sítě produktu IBM MQ a způsob, jakým jsou data sítě produktu IBM MQ komprimovaná do záznamů SSL/TLS.

Produkt MQIPT zachová balení dat sítě produktu IBM MQ v záznamech SSL/TLS bez rozdělení nebo kombinování těchto dat. Pokud jiné mosty SSL/TLS nezachovají záznamy SSL/TLS přesně, mohou způsobit selhání kanálů produktu IBM MQ s chybovými zprávami:

```
AMQ9638: SSL communications error for channel
AMQ9208: Error on receive from host
```

Režim serveru proxy protokolu

Přenosová cesta MQIPT může být konfigurována v režimu serveru proxy SSL/TLS jako alternativa k přemostění SSL/TLS. V tomto režimu postoupila přenosová cesta pouze data SSL/TLS mezi dvěma koncovými body IBM MQ ; nepodílí se na navázání komunikace SSL/TLS a nevyžaduje žádné digitální certifikáty.

Režim serveru proxy SSL/TLS můžete použít v případech, kdy kanály IBM MQ , které komunikují prostřednictvím produktu MQIPT , jsou již nakonfigurovány pro komunikaci SSL/TLS a chcete použít produkt MQIPT k jinému účelu, například směrování připojení pomocí bran firewall nebo omezení sady povolených připojení pomocí uživatelské procedury zabezpečení. Při spuštění v režimu serveru proxy

SSL/TLS produkt MQIPT kontroluje, zda počáteční pakety SSL/TLS přijaté z nového připojení jsou platné před předáním paketů do místa určení.

IBM MQ podporuje režim serveru proxy SSL/TLS s MQIPT nebo jakýmkoli jiným serverem proxy SSL/TLS

Podpora více certifikátů IBM MQ s produktem MQIPT

Produkt IBM MQ 8.0a později podporuje použití více certifikátů ve stejném správci front s použitím štítku certifikátu na kanál zadaný pomocí atributu **CERTLABL** v definici kanálu. Příchozí kanály správci front (například připojení k serveru nebo příjemce) se spoléhají na zjištění názvu kanálu pomocí protokolu SNI (TLS Server Name Indication), aby mohl předložit správný certifikát od správce front.

Pokud se kanál připojuje k cílovému správci front prostřednictvím MQIPTa přenosová cesta MQIPT má nastaveny jak **SSLServer** , tak **SSLClient** , existují mezi koncovými body dvě samostatné relace TLS a data SNI neprojdou přes přerušení relace. Zabráníte tak použití certifikátu na kanál v cílovém správci front pro připojení TLS mezi produktem MQIPT a správcem front. Chcete-li v cílovém správci front použít certifikát na kanál, pro připojení TLS, které projde přes MQIPT, musí trasa MQIPT použít režim serveru proxy SSL/TLS, který předává všechny řídicí toky TLS, včetně názvu SNI.

Certifikáty, které se používají pro připojení TLS, která jsou ukončeny nebo iniciovány produktem MQIPT , lze konfigurovat jednotlivě pro každou trasu, například pomocí vlastností směrování **SSLServerSiteLabel** a **SSLClientSiteLabel** .

CipherSuites podporované produktem MQIPT

V následující tabulce jsou uvedeny informace o tom, které šifrovací sady CipherSuites jsou podporovány produktem MQIPT a které jsou standardně povoleny.

Ve výchozím nastavení je povolena pouze podmnožina CipherSuites . CipherSuites založené na několika algoritmech, které jsou považovány za nezabezpečené, jsou zakázány JRE. Pokud jste si vědomi potenciálních rizik, ale stále potřebujete použít některý z těchto CipherSuites, můžete přidat podporu pro zakázanou sadu CipherSuite podle postupu uvedeného v tématu “Povolení zamítnutých protokolů a CipherSuites v produktu MQIPT” na stránce 964.

CipherSuite	Standardně povoleno
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_danon_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	V 9.1.4 Ano

CipherSuite	Standardně povoleno
SSL_DHE_DSS_WITH_AES_128_CBC_SHA256	V 9.1.4 Ano
SSL_DHE_DSS_WITH_AES_128_GCM_SHA256	V 9.1.4 Ano
SSL_DHE_DSS_WITH_AES_256_CBC_SHA	V 9.1.4 Ano
SSL_DHE_DSS_WITH_AES_256_CBC_SHA256	V 9.1.4 Ano
SSL_DHE_DSS_WITH_AES_256_GCM_SHA384	V 9.1.4 Ano
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	V 9.1.4 Ano
SSL_DHE_RSA_WITH_AES_128_CBC_SHA256	V 9.1.4 Ano
SSL_DHE_RSA_WITH_AES_128_GCM_SHA256	V 9.1.4 Ano
SSL_DHE_RSA_WITH_AES_256_CBC_SHA	V 9.1.4 Ano
SSL_DHE_RSA_WITH_AES_256_CBC_SHA256	V 9.1.4 Ano
SSL_DHE_RSA_WITH_AES_256_GCM_SHA384	V 9.1.4 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	

CipherSuite	Standardně povoleno
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	
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_WITHNULL_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	

CipherSuite	Standardně povoleno
SSL_KRB5_WITH_RC4_128_SHA	
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	
SSL_RSA_EXPORT_WITH_RC4_40_MD5	
SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA (poznámka 1)	
SSL_RSA_FIPS_WITH_DES_CBC_SHA (Poznámka 1)	
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
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	

Poznámka:

1. Přestože je tato sada CipherSuite podporována pro kompatibilitu s předchozími verzemi, není již kompatibilní se standardem FIPS a jeho použití by mělo být zabráněno.

IBM MQ CipherSpecs a MQIPT CipherSuites

Následující tabulka zobrazuje vztah mezi CipherSpecs podporovaným produktem IBM MQ a CipherSuites , který je podporován produktem MQIPT.

Tabulka také uvádí verzi protokolu, kterou produkt IBM MQ očekává, že každá CipherSpec bude použita.

IBM MQ CipherSpec jedinečně určuje šifrovací algoritmus a také verzi zabezpečeného soketového protokolu, která se má použít. Některé IBM MQ CipherSpecs se liší pouze verzí protokolu, takže není dostatečné nakonfigurovat sadu CipherSuite samostatně. Při navázání komunikace protokolu SSL/TLS je vyjednána nejvyšší podporovaná verze protokolu zabezpečeného soketu podporovaná oběma stranami a poté vybere sadu CipherSuite ze sady vzájemně povolených šifer.

Například přenosová cesta SSLClient s `SSLClientCipherSuites=SSL_RSA_WITH_3DES_EDE_CBC_SHA` může vyjednat 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 vyjednat tuto CipherSuite přes TLS 1.2, ale produkt IBM MQ nepodporuje tuto sadu CipherSuite přes TLS 1.2. Z tohoto důvodu jsou pro cesty SSLClient pravděpodobně příčinou chyby AMQ9616 nebo AMQ9631 ve správci front.

Chcete-li se těmto chybám vyhnout na trasách SSLClient, nastavte vlastnost cesty **`SSLClientProtocols`** na příslušnou hodnotu pro požadovanou hodnotu CipherSpec. V některých případech může být také nutné omezit sadu protokolů na straně serveru s použitím vlastnosti směrování

produktu **SSLServerProtocols** . Použijte verzi protokolu uvedenou v tabulce, abyste určili správné nastavení pro tyto vlastnosti přenosové cesty.

Tento problém se týká zejména následujících sad CipherSuites a CipherSpecs pro cesty SSLClient:

- SSL_RSA_WITH_3DES_EDE_CBC_SHA, který 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 jedinou přenosovou cestu MQIPT SSLClient k tunelu více IBM MQ kanálů, které používají různé specifikace CipherSpecs, zajistěte, aby všechny kanály měly CipherSpecs , které používají stejnou verzi zabezpečeného protokolu soketů jako sobě a že jste produkt **SSLClientProtocols** nastavili pro použití této verze jednoduchého protokolu.

Další informace o produktu IBM MQ CipherSpecsviz téma Povolení specifikace 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_WITHNULL_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

IBM MQ CipherSpec	MQIPT CipherSuite	Verze protokolu
FIPS_WITH_3DES_EDE_CBC_SHA (poznámka 1)	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	SSLv3
FIPS_WITH_DES_CBC_SHA (poznámka 1)	SSL_RSA_FIPS_WITH_DES_CBC_SHA	SSLv3
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
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
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

SSL/TLS handshake in MQIPT

Proces navázání komunikace pomocí protokolu SSL/TLS probíhá při počátečním požadavku na připojení mezi klientem a serverem protokolu SSL/TLS při ověřování a dohadování sady CipherSuites .

Všechny podporované SSL/TLS CipherSuites (viz “Podpora SSL/TLS v MQIPT” na stránce 941), s výjimkou anonymních CipherSuites, vyžadují ověření serveru a umožňují ověření klienta; server může být nakonfigurován pro požadování ověření klienta. Měli byste se vyhnout použití anonymních CipherSuites , protože neposkytují žádné záruky ohledně identity vzdáleného peeru. Je možné, aby útok typu man-in-the-middle zachytil anonymní připojení SSL/TLS bez vašich znalostí. Anonymní šifrovací sady CipherSuites používejte pouze u důvěryhodných interních sítí a pouze v případě, že jste připraveni přijmout riziko zachycení dat.

Ověření rovnocenného partnera 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), doba platnosti certifikátu. Certifikáty jsou podepsány certifikační autoritou, certifikáty těchto orgánů se nazývají certifikáty podepisujících subjektů. Certifikát následovaný jedním nebo více certifikáty podepisujících subjektů tvoří řetěz certifikátů. Řetěz certifikátů je charakterizován skutečností, že počínaje prvním certifikátem (certifikát serveru) může být podpis každého certifikátu v řetězu ověřen pomocí veřejného klíče obsaženého v dalším certifikátu podepsaného.

Když je ustanoveno zabezpečené připojení, které vyžaduje autentizaci serveru, server odešle klientovi certifikát řetězu, aby prokázal svou totožnost. Klient SSL/TLS bude provádět připojení k serveru pouze v případě, že může ověřit server, například ověřit podpis certifikátu serveru. Aby mohl klient SSL/TLS ověřit tento podpis, musí důvěřovat samotnému serveru nebo alespoň jednomu z podepisujících subjektů v řetězu certifikátů poskytovaného serverem. Certifikáty důvěryhodných serverů a podepisujících subjektů musí být udržovány na straně klienta, aby bylo možné provést toto ověření.

Klient SSL/TLS prověřuje řetězec certifikátu serveru, počínaje certifikátem serveru. Klient má za to, že podpis certifikátu serveru je platný za následujících okolností:

- Certifikát serveru se nachází v úložišti důvěryhodných serverů nebo certifikátů podepsaných subjektů.
- Certifikát podepisujícího subjektu v řetězu lze ověřit na základě jeho úložiště důvěryhodných certifikátů podepsaného.

V druhém případě klient SSL/TLS kontroluje, zda je řetěz certifikátů skutečně správně podepsán, z důvěryhodného certifikátu podepsaného na certifikát serveru daného serveru. Každý certifikát zahrnutý v tomto procesu je také zkoumán za správnost formátu a data platnosti. Pokud některá z těchto kontrol selže, je připojení k serveru odmítnuto. Po ověření certifikátu serveru klient používá veřejný klíč vložený v tomto certifikátu v dalších krocích protokolu SSL/TLS. Připojení SSL/TLS lze navázat pouze tehdy, má-li server skutečně odpovídající soukromý klíč.

Ověření klienta se provádí stejným postupem: pokud server SSL/TLS vyžaduje ověření klienta, klient odešle na server řetězec certifikátů, aby prokázal svou identitu. Server ověřuje řetěz na základě svého úložiště důvěryhodných serverů a certifikátů podepisujících subjektů. Po ověření certifikátu klienta server používá veřejný klíč, který je vložen do tohoto certifikátu v dalších krocích protokolu SSL/TLS. Připojení SSL/TLS může být vytvořeno pouze v případě, že má klient skutečně odpovídající soukromý klíč.

Nejnovější verze protokolů TLS zajišťují vysoce zabezpečenou komunikaci (zabezpečení SSL a starší protokoly TLS jsou považovány za nezabezpečené). Protokol však funguje na základě informací poskytnutých aplikací. Pouze v případě, že informační základna je také udržována bezpečně celkový cíl bezpečné komunikace může být dosaženo. Je-li například ohroženo úložiště důvěryhodných serverů a certifikátů podepisujících subjektů, můžete vytvořit zabezpečené připojení k velmi nezabezpečenému komunikačnímu partnerovi.

Implementace protokolu SSL/TLS MQIPT

SSL 3.0 a TLS 1.0, 1.1a 1.2 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 .

V 9.1.4 MQIPT může také použít šifrovací hardwarová úložiště klíčů, která podporují standard rozhraní PKCS#11 Cryptographic Token Interface. Produkt MQIPT používá balík IBM Java Secure Socket Extension (JSSE).

Produkt MQIPT může působit 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 trasa MQIPT jednala jak jako klient, tak i server. V takovém případě je při použití funkce režimu serveru proxy SSL/TLS obvykle lepší výkon.

Je-li produkt MQIPT konfigurován pro režim serveru proxy SSL/TLS, předává data protokolu SSL/TLS pouze mezi dvěma koncovými body; nepodílí se na navázání komunikace SSL/TLS a nevyžaduje žádné digitální certifikáty.

MQIPT nepředává data SNI (Server Name Indication), která jsou přijata na příchozím připojení TLS, přes odchozí připojení TLS. To znamená, že certifikáty pro jednotlivé kanály určené pomocí atributu

kanálu produktu **CERTLABL** nelze použít pro připojení TLS mezi produktem MQIPT a správcem cílové fronty. Chcete-li v cílovém správci front použít certifikát na kanál, pro připojení TLS, které projde přes MQIPT, musí trasa MQIPT použít režim serveru proxy SSL/TLS, který předává všechny řídicí toky TLS, včetně názvu SNI. Další informace o použití více certifikátů ve správci front s produktem MQIPTnaleznete v příručce “Podpora více certifikátů IBM MQ s produktem MQIPT” na stránce 943.

Každá cesta MQIPT může být nezávisle konfigurována s vlastní sadou vlastností SSL/TLS. Další podrobnosti najdete v tématu MQIPT Vlastnosti přenosové cesty .

Šifrování hesla svazku klíčů v produktu MQIPT

Zašifrujte heslo použité k otevření souboru svazku klíčů, nebo pro přístup k kryptografickému hardwaru používanýmu MQIPT příkazem **mqiptPW** . Šifrované heslo lze použít kteroukoli z následujících vlastností: **SSLClientKeyRingPW**, **SSLClientCAKeyRingPW**, **SSLServerKeyRingPW**a **SSLServerCAKeyRingPW**. Toto téma popisuje správný způsob uložení hesla svazku klíčů pro použití produktem MQIPT.

Poskytovaná služba **mqiptkeyman** (iKeyman) pro soubor stash není podporována produktem MQIPT. Místo použití souboru pro dočasné ukládání musíte použít příkaz **mqiptPW** k uložení šifrovaného hesla.

Ve verzích starších než IBM MQ 9.1.5jsou hesla ke svazku klíčů pro použití produktem MQIPT uložena v souborech, na které se odkazuje libovolná z vlastností produktu **SSL*KeyRingPW** .

V 9.1.5 V produktu IBM MQ 9.1.5zašifrujte hesla svazku klíčů pro použití příkazem MQIPT pomocí příkazu **mqiptPW** a nastavte hodnotu vlastností **SSL*KeyRingPW** na šifrované 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.

Metoda šifrování hesel úložiště klíčů, která jsou k dispozici ve starších verzích produktu MQIPT než IBM MQ 9.1.5 , je sice zamítnuta, ale lze ji přesto použít. Chcete-li zlepšit ochranu hesel klíčových řetězců, znovu zašifrujte všechna hesla klíčových řetězců, která byla dříve zašifrována, pomocí nejnovější metody ochrany.

Chcete-li zašifrovat heslo svazku klíčů pro použití produktem MQIPT, postupujte podle kroků uvedených v tématu Šifrování uložených hesel.

Musíte použít heslo `mqiptSample` k otevření jednoho z ukázkových souborů svazku klíčů, které jsou dodány v podadresáři `samples/ssl` instalačního adresáře produktu MQIPT .

Výběr certifikátů ze souboru svazku klíčů v produktu MQIPT

Je možné mít více než jeden osobní certifikát uložený ve stejném souboru svazku klíčů nebo kryptografický token hardwaru. Vlastnosti **SSLClientSite*** lze použít na straně klienta k výběru certifikátu, který se má odeslat na server pro ověření, a vlastnosti **SSLServerSite*** lze použít na straně serveru k výběru certifikátu, který má být odeslán klientovi pro ověření.

Pomocí těchto vlastností lze vybrat certifikát na základě jeho rozlišujícího názvu (DN). Alternativně lze jmenovku certifikátu použít k výběru certifikátu pomocí vlastností **SSLServerSiteLabel** a **SSLClientSiteLabel** .

Nastavení důvěryhodnosti v produktu MQIPT

Svazek klíčů obsahuje osobní certifikát, který obsahuje certifikát podepisujícího subjektu nebo řetězec certifikátů podepisujících subjektů.

Existují dva typy svazků klíčů, které používá produkt MQIPT:

Svazek klíčů vydavatele certifikátů (CA)
Tento svazek klíčů obsahuje důvěryhodné certifikáty CA používané k ověření certifikátů náležících ke vzdálenému peeru. Tyto certifikáty CA pomáhají určit, zda je vzdálený peer důvěryhodný. Produkt MQIPT podporuje jak soubory svazku klíčů PKCS #12 , tak kryptografické hardwarové úložiště klíčů podporující rozhraní PKCS #11 pro ukládání certifikátů CA. Soubory svazku klíčů MQIPT CA jsou identifikovány vlastnostmi směrování **SSLClientCAKeyRing** a **SSLServerCAKeyRing** . Použití

kryptografického hardwaru pro přístup k certifikátům CA je zpřístupněno nastavením vlastností **SSLClientCAKeyRingUseCryptoHardware** a **SSLServerCAKeyRingUseCryptoHardware** .

Klíčový řetězec CA na straně klienta SSL/TLS by měl obsahovat seznam důvěryhodných certifikátů CA, které budou použity k ověření certifikátu odeslaného ze serveru. Je-li přenosová cesta serveru SSL konfigurována pro ověření klienta, měl by svazek klíčů CA na straně serveru SSL/TLS 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 MQIPT používá k identifikaci sebe sama se vzdáleným peerem. Při generování certifikátu podepsaného držitelem nebo požadavku certifikátu podepsaného (CA) certifikátu byste tak měli učinit pomocí svazku klíčů osobního certifikátu. Produkt MQIPT podporuje jak soubory svazku klíčů PKCS #12 , tak kryptografické hardwarové úložiště klíčů podporující rozhraní PKCS #11 pro ukládání osobních certifikátů. V produktu MQIPTjsou soubory svazku klíčů osobního certifikátu identifikovány vlastnostmi směrování **SSLClientKeyRing** a **SSLServerKeyRing** . Použití kryptografického hardwaru pro přístup k osobním certifikátům je zpřístupněno nastavením vlastností **SSLClientKeyRingUseCryptoHardware** a **SSLServerKeyRingUseCryptoHardware** .

Klíč svazku klíčů na straně serveru SSL/TLS by měl obsahovat osobní certifikát serveru MQIPT . Je-li na cestě klienta SSL vyžadováno ověření klienta, měl by klíč klienta na straně klienta SSL/TLS obsahovat osobní certifikát klienta.

Pokud potřebujete ověření klienta, je třeba povolit vlastnost **SSLServerAskClientAuth** na straně serveru. Soubor svazku klíčů na straně klienta by měl obsahovat osobní certifikát klienta. Klíčový řetězec MQIPT na straně serveru, který je identifikován vlastností **SSLServerCAKeyRing** , by měl obsahovat seznam důvěryhodných certifikátů CA, které budou použity pro ověření klienta.

Pokud pro přenosovou cestu nenakonfigurujete svazek klíčů CA, produkt MQIPT vyhledá certifikáty CA v souboru svazku klíčů osobního certifikátu namísto toho, je-li konfigurován. Například, pokud není nastavena žádná hodnota pro **SSLServerCAKeyRing**, MQIPT vyhledá certifikáty CA v souboru svazku identifikovaném pomocí **SSLServerKeyRing**.

Jako alternativu k používání certifikátů podepsaných důvěryhodnou certifikační autoritou můžete použít certifikáty podepsané sebou samým. You can find an example of a self-signed certificate in the `sslSample.pfx` sample key ring file provided with MQIPT in the `samples/ssl` subdirectory. Chcete-li otevřít ukázkové soubory svazku klíčů PKCS#12 , musíte použít heslo `mqiptSample`.

Certifikáty podepsané svým držitelem mohou být užitečné ve scénářích testu, kde musíte zajistit konektivitu SSL/TLS, aniž byste museli platit CA pro certifikát. Certifikáty podepsané sebou samým byste však neměli používat v produkčních prostředích. Chcete-li vytvořit certifikát podepsaný CA, přečtěte si téma Vytvoření souboru svazku klíčů.

Ke správě digitálních certifikátů a úložišť klíčů můžete použít obslužný program s názvem **mqiptkeyman**, který se dodává spolu s produktem MQIPT. Pokyny k instalaci a další informace naleznete v příručce “mqiptKeyman a mqiptKeycmd v MQIPT” na stránce 955 .

Musíte chránit všechny soubory svazku klíčů a soubory hesel tak, že použijete funkce zabezpečení operačního systému, abyste zabránili neoprávněnému přístupu k nim.

Testování SSL/TLS v MQIPT

Připojení SSL/TLS můžete otestovat pomocí příkladů uvedených v této dokumentaci.

Popis různých scénářů naleznete v tématu Začínáme s produktem IBM MQ Internet Pass-Thru . Zejména se podívejte na následující úlohy:

- Ověřování serveru SSL/TLS
- Ověřování klienta SSL/TLS
- Spuštění produktu MQIPT v režimu serveru proxy SSL/TLS
- Spuštění produktu MQIPT v režimu serveru proxy SSL/TLS se správcem zabezpečení

Chcete-li otestovat, že konfigurace protokolu SSL/TLS pracuje správně, můžete použít certifikáty podepsané sebou samým. Certifikáty podepsané svým držitelem jsou užitečné v testovacích scénářích, abyste mohli zajistit konektivitu SSL/TLS bez nutnosti platit certifikační autority (CA) pro certifikát. Podrobnosti viz Vytvoření testovacích certifikátů .

You can find an example of a self-signed certificate in the `sslSample.pfx` sample key ring file provided with MQIPT in the `samples/ssl` subdirectory. Chcete-li otevřít ukázkové soubory svazku klíčů PKCS #12 , musíte použít heslo `mqiptSample`. Vzorové certifikáty jsou poskytnuty pro vaše pohodlí během testování. Avšak soukromé klíče vzorového certifikátu jsou známé všem uživatelům produktu MQIPT . To znamená, že je nespolehlivé a mělo by být použito pouze v testovacím prostředí.

V produkčních prostředích byste neměli používat žádné certifikáty podepsané svým držitelem, ať už se jedná o ukázkové certifikáty či nikoli. Místo toho získejte certifikát podepsaný CA od důvěryhodné CA. Chcete-li vytvořit certifikát podepsaný CA, přečtěte si téma Vytvoření souboru svazku klíčů.

Při vytváření nebo požadování certifikátu byste měli zvážit, který typ klíče, velikost klíče a algoritmus digitálního podpisu jsou vhodné pro vaše potřeby zabezpečení. Další informace viz “Aspekty digitálního certifikátu pro produkt MQIPT” na stránce 957.

Certifikáty a technologie správy certifikátů jsou k dispozici od řady dodavatelů třetích stran.

Chybové zprávy SSL/TLS v MQIPT

Selhání navázání komunikace jsou zaprotokolovány do protokolu připojení MQIPT ve formě výjimek JSSE.

Další informace viz téma “Protokoly připojení v produktu MQIPT” na stránce 979. Následující tabulka popisuje různé výjimky, pravděpodobnou příčinu a odpovídající akci k vyřešení selhání.

Výjimky certifikátu se obvykle vztahují k certifikátům na vzdáleném konci připojení.

Pokud se chyba vztahuje k certifikátu klienta nebo správce front produktu IBM MQ , termín *soubor svazku klíčů* obsahuje úložiště klíčů produktu IBM MQ vzdáleného partnera.

V produktu MQIPTjsou certifikáty CA uloženy v souboru svazku klíčů CA, který je identifikován vlastnostmi směrování **SSLClientCAKeyRing** a **SSLServerCAKeyRing** . Pokud nejsou nastaveny vlastnosti přenosové cesty klíče CA, odpovídající soubor svazku osobních klíčů (odkazovaný buď ve vlastnosti **SSLClientKeyRing** nebo **SSLServerKeyRing**) je prohledáván pro certifikáty CA.

Výjimka	**Příčina**	**Akce**
CertificateException	Certifikát není důvěryhodný, protože je podepsán CA, který není v klíčovém svazku CA.	Zkontrolujte, zda jsou všechny potřebné certifikáty CA obsaženy v souboru svazku klíčů CA. Pomocí nástroje pro správu klíčů produktu IBM dodaného s produktem MQIPT přidejte všechny chybějící certifikáty CA, přičemž se postarejte o získání kopie každého certifikátu CA z důvěryhodného zdroje.
Výjimka CertificateExpired	1. Vypršela platnost certifikátu: **notAfter** uplynulo jeho datum. 2. Systémové hodiny jsou nastaveny nesprávně.	1. Získejte nový certifikát a vložte jej do souboru svazku klíčů. Pokud certifikát náleží certifikační autoritě, umístěte nový certifikát do souboru svazku klíčů CA. 2. Zkontrolujte, zda je systémový čas UTC nastaven na správný čas.

Výjimka	Příčina	Akce
CertificateNotYetValidVýjimka	1. Certifikát se používá předčasně: jeho datum **notBefore** ještě nedorazilo. 2. Systémové hodiny jsou nastaveny nesprávně.	1. Zkontrolujte, zda byl certifikát vygenerován a správně podepsán. Pokud vaše organizace provozuje svou vlastní certifikační autoritu, časová základna systému UTC pro CA může být chybná. 2. Zkontrolujte, zda je systémový čas UTC nastaven na správný čas.
Výjimka CertificateParsing	1. Certifikát obsahuje neplatná data DER. 2. Certifikát používá nepodporované funkce DER.	Ujistěte se, že certifikát byl správně vygenerován a lze jej zobrazit v nástroji IBM Key Management dodaném s MQIPT. Uvažte získání nového certifikátu s menším počtem rozšíření certifikátu.
Výjimka CertificateRevoked	Kontrola odvolání certifikátů je povolena a byl nalezen certifikát, který má být odvolán.	Certifikát by neměl být důvěryhodný. Získejte náhradní certifikát a ujistěte se, že nový certifikát a jeho soukromý klíč se nacházejí v souboru svazku klíčů.
CertPathBuilderException	Řetěz certifikátů nebyl podepsán uznávanou certifikační autoritou.	1. Pokud používáte certifikáty podepsané certifikační autoritou (CA), zkontrolujte, zda jsou v souboru svazku klíčů CA přítomna všechna kořenová CA a zprostředkující certifikáty CA. 2. Pokud používáte certifikáty podepsané sebou samým, ujistěte se, že jste extrahovali kopii veřejné části vzdáleného certifikátu a přidali ji do souboru svazku klíčů CA. Vyvarujte se použití certifikátů s automatickým podpisem v produkčních prostředích.

Výjimka	Příčina	Akce
Výjimka CertStore Výjimka KeyStore	Došlo k chybě při čtení certifikátu z svazku klíčů z jednoho z následujících důvodů: 1. Soubor svazku klíčů je poškozen. 2. Soubor svazku klíčů chybí. 3. Uložené heslo se neshoduje s heslem souboru klíčového řetězce. 4. Je-li přenosová cesta nakonfigurována pro použití kryptografického hardwaru, produkt MQIPT se nemohl připojit k kryptografickému hardwaru.	1. Ujistěte se, že soubor svazku klíčů lze číst a že všechny certifikáty lze zobrazit pomocí nástroje pro správu klíčů produktu IBM . 2. Zkontrolujte, že všechny vlastnosti přenosové cesty klíče odkazují na správný název souboru. 3. Zkontrolujte, zda je uložené heslo souboru svazku klíčů správné. Použijte nástroj **mqiptPW** k uložení správného hesla. 4. Je-li přenosová cesta konfigurována pro použití kryptografického hardwaru, zkontrolujte následující: • Soubor vlastností zabezpečení produktu Java určuje, že je nainstalován poskytovatel zabezpečení IBMPKCS11Impl . • Soubor vlastností zabezpečení produktu Java obsahuje úplný název konfiguračního souboru, který se používá k inicializaci poskytovatele zabezpečení IBMPKCS11Impl . • Konfigurační soubor, který se používá k inicializaci poskytovatele zabezpečení IBMPKCS11Impl , je platný.
SSLException: K dispozici není žádný certifikát nebo klíč k dispozici šifrovací sady 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 sady CipherSuites vyžadují certifikát s veřejným klíčem RSA.	Otevřete soubor svazku klíčů pomocí nástroje Správa klíčů IBM . V zobrazení Osobní certifikáty vyberte postupně každý certifikát a zobrazte jej. Klepněte na volbu **Zobrazit podrobnosti** a přejděte do části Veřejný klíč předmětu a prohlédněte si typ veřejného klíče. Poté zkontrolujte vlastnosti směrování produktu MQIPT **SSLClientCipherSuites** a **SSLServerCipherSuites** , abyste se ujistili, že je povoleno příslušné CipherSuites .

Výjimka	Příčina	Akce
SSLException: Není společné žádné šifrovací sady SSLHandshakeException: Žádné šifrovací sady nejsou společné.	Navazování komunikace se nepodařilo dohodnout na sadě CipherSuite , protože mezi sadami povolených CipherSuites na obou koncích připojení neexistuje žádné překrytí. Zejména odchozí připojení produktu IBM MQ povoluje pouze jednoduchou šifru, takže přenosové cesty SSLServer MQIPT se s touto chybou pravděpodobně setkají velmi pravděpodobně. K této chybě může také dojít, jsou-li splněny všechny tři následující podmínky: • na trase není zadána žádná sada CipherSuite . • v klíčovém kruhu konfigurovaném pro přenosovou cestu nelze nalézt žádný vhodný certifikát serveru. • anonymní CipherSuites jsou zakázány	Zkontrolujte seznam povolených CipherSuites ve vlastnostech trasy MQIPT **SSLClientCipherSuites** a **SSLServerCipherSuites** . Zvažte povolení dalších CipherSuites. Nahlédněte do poskytnuté tabulky, abyste určili správné CipherSuites , které chcete povolit pro každou hodnotu CipherSpec kanálu produktu IBM MQ . Není-li na trase zadána žádná sada CipherSuite , zkontrolujte, zda vlastnosti směrování klíčových řetězců odkazují na správný soubor svazku klíčů a že svazek klíčů obsahuje osobní certifikát, který může produkt MQIPT použít. Je-li přenosová cesta konfigurována pro použití kryptografického 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 certifikát a aplikace správy klíčů, které jsou již obeznámeni s uživateli produktu IBM MQ . Příkazy **mqiptKeyman** a **mqiptKeycmd** mohou být použity ke správě symetrických a asymetrických klíčů, digitálních certifikátů a požadavků na certifikáty v souborech svazku klíčů používaných produktem IBM MQ Internet Pass-Thru. Tyto soubory lze také použít ke správě samotných souborů svazku klíčů.

mqiptKeyman používá termín *databáze klíčů* k odkazování na soubor svazku klíčů; tyto termíny jsou synonymní.

Produkt **mqiptKeyman** lze spustit ve dvou režimech, grafickém uživatelském rozhraní (GUI) a rozhraní příkazového řádku (CLI-command-line interface). Pomocí příkazu **mqiptKeyman** spusťte grafické rozhraní iKeyman a příkaz **mqiptKeycmd** ke spuštění rozhraní CLI iKeyman .

Ekvivalentní příkazy pro správu certifikátů v produktu IBM MQ jsou **strmqikm** ke spuštění grafického uživatelského rozhraní iKeyman a produktu **runmqckm** ke spuštění rozhraní CLI iKeyman . Příkazy IBM MQ jsou popsány v části Použití produktů **runmqckm**, **runmqakm**a **strmqikm** ke správě digitálních certifikátů.

Požadovaný formát souboru svazku klíčů pro MQIPT

Při vytváření souborů svazku klíčů pro použití v produktu MQIPTje nutné použít formát souboru PKCS #12 :

- V grafickém rozhraní vyberte PKCS#12 v poli **Typ databáze klíčů** při vytváření souboru svazku klíčů.
- V rozhraní CLI zahrňte parametr `-type pkcs12` do příkazu `mqiptKeycmd -keydb -create` .

V 9.1.4 Produkt MQIPT může také přistupovat k certifikátům uloženým v kryptografickém hardwaru, který podporuje rozhraní PKCS #11 . Toto rozhraní lze také použít ke správě certifikátů na hardwaru

PKCS #11 . Další informace viz téma “Použití kryptografického hardwaru PKCS #11 v příručce MQIPT” na stránce 965.

Šifrování hesla svazku klíčů pro MQIPT

Po vytvoření souboru svazku klíčů musíte zašifrovat heslo svazku klíčů ve formátu, který produkt MQIPT může použít pro přístup k souboru. Informace o tomto tématu viz “Šifrování hesla svazku klíčů v produktu MQIPT” na stránce 950 .

Všimněte si, že poskytovaná služba souboru pro dočasné ukládání není produktem MQIPTpodporována. Musíte použít příkaz **mqiptPW** k zašifrování hesla klíčového řetězce místo použití souboru stash.

Příklady příkazového řádku

Rozhraní CLI používá stejnou syntaxi jako příkaz IBM MQ **runmqckm** . Přidejte požadované parametry do **mqiptKeycmd**, jak ukazuje následující příklady:

- 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:

```
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 se postarejte o to, abyste zvolili šifrovací algoritmus veřejného klíče, velikost klíče a algoritmus digitálního podpisu, které odpovídají potřebám zabezpečení vaší organizace. Další informace viz “Aspekty digitálního certifikátu pro produkt MQIPT” na stránce 957.

  Tento příklad používá certifikát podepsaný (svým) držitelem, který je vhodný pro testovací účely. V produkčním prostředí byste však měli namísto toho používat certifikát podepsaný vydavatelem certifikátů.

  Všimněte si, že MQIPT v2.0 a starší verze nepodporují digitální podpisy SHA-2 , takže tento certifikát není vhodný pro navázání zabezpečených soketových připojení k předchozím verzím produktu MQIPT ; je zapotřebí starší podpisový algoritmus, jako např. SHA1WithRSA.

- Chcete-li vytvořit žádost o certifikát pro certifikát podepsaný CA pro produktivní 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 se postarejte o to, abyste zvolili šifrovací algoritmus veřejného klíče, velikost klíče a algoritmus digitálního podpisu, které odpovídají potřebám zabezpečení vaší organizace. Další informace viz “Aspekty digitálního certifikátu pro produkt MQIPT” na stránce 957.

- Chcete-li přijmout soubor osobního certifikátu podepsaného CA `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 CA certifikátu 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 digitálního certifikátu pro produkt MQIPT

Mezi body, které je třeba vzít v úvahu, patří velikost klíče certifikátu, výběr odpovídajícího algoritmu digitálního podpisu certifikátu a digitální certifikát a certifikát CipherSuite compatibilityDigital a kompatibilita CipherSuite .

Aspekty velikosti klíče certifikátu pro MQIPT

Velikost veřejného klíče závisí na zásadě zabezpečení vaší organizace a závisí na použitém šifrovacím algoritmu. Obecně platí, že větší velikost klíče je bezpečnější. V následující tabulce jsou uvedeny minimální velikosti klíče, které byste měli použít:

algoritmus	**Minimální velikost klíče (bity)**
Eliptická křivka	256
RSA	2048

Uveďte velikost klíče certifikátu, když vytváříte certifikát nebo žádost o certifikát.

- Při použití příkazu **mqiptKeycmd** CLI určuje parametr **-size** velikost klíče.
- Použijete-li grafické uživatelské rozhraní produktu **mqiptKeyman** , pole **Velikost klíče** v okně Vytvoření certifikátu uvádí velikost klíče.

Výběr odpovídajícího algoritmu digitálního podpisu certifikátu

Aby se zabránilo padělání digitálních certifikátů, je důležité použít silný algoritmus digitálního podpisu. Když vytváříte nebo požadujete certifikát, drejte si pozor na správný algoritmus.

Měli byste se vyhnout používání starých algoritmů digitálních podpisů 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 na bázi SHA-2 , jako je SHA-256 s RSA (SHA256WithRSA).

Verze produktu MQIPT starší než verze 2.1 však nepodporují digitální podpisy SHA-2 , takže pro interoperabilitu s předchozími vydáními MQIPT použijte algoritmus digitálního podpisu SHA1WithRSA . Měli byste však naplánovat upgrade starších verzí produktu MQIPT a ukončení použití digitálních podpisů MD5 a SHA-1 .

- Pokud používáte příkaz **mqiptKeycmd** CLI, parametr **-sig_alg** určuje algoritmus digitálního podpisu.
- Při použití grafického uživatelského rozhraní produktu **mqiptKeyman** určuje algoritmus **Signature Algorithm** v okně Vytvoření certifikátu algoritmus digitálního podpisu.

Digitální certifikát a kompatibilita CipherSuite v produktu MQIPT

Ne všechny CipherSuites lze použít se všemi digitálními certifikáty. K dispozici jsou různé typy sady CipherSuite, seskupené podle předpony názvu CipherSuite . Každý typ sady CipherSuite klade různá omezení na typ digitálního certifikátu, který lze použít. Tato omezení se vztahují na všechna připojení SSL/TLS MQIPT , ale jsou zvláště důležitá pro uživatele šifrování Elliptic Curve. Při provádění navázání komunikace zabezpečení SSL produkt MQIPT automaticky vybere osobní certifikát, aby identifikoval sám sebe, který je vhodný pro vyjednávanou sadu CipherSuite. Ve většině případů produkt MQIPT automaticky spolupracuje se vzdáleným peerem. Nicméně v některých scénářích může být nutné použít ke spolupráci se vzdáleným systémem IBM MQ konkrétní MQIPT CipherSuite . Aplikace **mqiptKeyman** dodávaná s produktem MQIPT je schopná vytvářet certifikáty a požadavky na 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. Poraďte se se svým lékařem o radu při vytváření jiných typů certifikátů.

Typ digitálního certifikátu, který má být použit, závisí na typu sady CipherSuite , kterou používáte:

- CipherSuites s názvy, které začínají SSL_ECDH_ECDSA_ a SSL_ECDHE_ECDSA_ vyžadují digitální certifikát s veřejným klíčem Elliptic Curve.
- CipherSuites s názvy obsahujícími *anan* jsou anonymní; nevyžadují digitální certifikát k identifikaci vzdáleného peeru. Takové CipherSuites se mohou vyvarovat režijních nákladů správy životního cyklu certifikátu v sítích, kde jsou použity alternativní prostředky ověření, ale obecně, se vyvarovat jejich použití v důsledku nedostatku ověření.
- Ostatní CipherSuites vyžadují digitální certifikát s veřejným klíčem RSA.

Poznámka: Nástroje **mqiptKeyman** a **mqiptKeycmd** nemohou vytvořit certifikáty nebo požadavky na certifikáty s veřejným klíčem Elliptic Curve. K tomuto účelu můžete použít příkaz **runmqakm** poskytnutý s IBM MQ . Příkaz **runmqakm** je popsán v části Použití produktů **runmqckm**, **runmqakm**a **strmqikm** ke správě digitálních certifikátů.

Uživatelská procedura certifikátu v produktu MQIPT

Účelem uživatelské procedury certifikátu je ověřit certifikát rovnocenného partnera SSL/TLS, který je přijat produktem MQIPT.

Můžete nakonfigurovat trasu MQIPT tak, aby se chovala jako klient SSL/TLS, když vytváří nové připojení a vystupuje jako server SSL/TLS, když přijme požadavek na připojení. Během procesu navázání komunikace SSL/TLS přijímá klient SSL/TLS certifikát typu peer ze serveru a certifikát lze použít k ověření serveru. Server SSL/TLS může také od klienta obdržet certifikát partnera a certifikát lze použít k ověření klienta.

Uživatelská procedura certifikátu se volá, když produkt MQIPT obdrží certifikát typu peer, což vám umožní provést další ověření. Všechny výjimky, které jsou zachyceny uživatelskou procedurou, jsou zachyceny produktem MQIPT a požadavek na připojení byl ukončen. Je proto dobrým zvykem pro výjezd zachytit všechny výjimky a předat zpět odpovídající návratový kód do MQIPT.

Ukázka je k dispozici pro zobrazení uživatelské procedury certifikátu, která může být implementována pro další informace viz téma Použití uživatelské procedury certifikátu k ověření serveru SSL/TLS.

Poznámka: MQIPT se spouští v jediném Java virtual machine , takže uživatelsky definovaná uživatelská procedura může ohrozit normální provoz MQIPT jedním z těchto způsobů:

- Ovlivněné systémové prostředky
- Generovat kritická místa
- Degrade výkon

Měli byste otestovat účinky výstupu certifikátu rozsáhle před implementací v produkčním prostředí.

Třída com.ibm.mq.ipt.exit.CertificateExit v produktu MQIPT

Abstraktní třída, která musí být implementována třídou, která je definována vlastností SSLExitName .

Třída obsahuje výchozí implementace pro spuštění uživatelské procedury a některé veřejné metody, které můžete volitelně potlačit, podle svých požadavků. Úplný seznam podporovaných metod je následující:

metody

public int init (IPTTrace)

Inicializační metoda je volána příkazem MQIPT při načítání uživatelské procedury produktem MQIPT a lze ji implementovat za účelem provedení libovolné inicializace uživatelské procedury; například načtení dat použitých během procesu ověření platnosti. Výchozí implementace nedělá nic.

public int refresh (IPTTrace)

Metoda obnovy je implementována, aby provedla aktualizaci jakýchkoli dat; například nové načtení všech dat pro disk, které se používají během procesu ověření platnosti. Tato metoda se volá, když administrátor produktu MQIPT vydal příkaz k aktualizaci. Výchozí implementace nedělá nic.

public void close (IPTTrace)

Metoda close je implementována za účelem provedení úklidu, pokud má být trasa zastavena nebo MQIPT se zavírá. Výchozí implementace nedělá nic.

public CertificateExitResponse validate (IPTTrace)

Metoda ověření se volá k provedení ověření rovnocenného certifikátu. Návratový objekt může být použit k předání informací zpět do MQIPT; například návratový kód a nějaký text, který lze přidat do protokolu připojení. Výchozí implementace vrací odpověď CertificateExits parametrem CertificateExitResponse.OK.

Podporované metody pro získání vlastností:

public int getListenerPort ()
načte port modulu listener směrování-jak je definováno vlastností ListenerPort .

veřejný řetězec getDestination()
načte adresu místa určení-jak je definováno vlastností Destination

public int getDestinationPort ()
Načte adresu portu cílového modulu listener-jak je definováno vlastností DestinationPort .

veřejný řetězec getClientIPAddress ()
načítá adresu IP klienta, který vytváří požadavek na připojení

public int getClientPortAddress()
načte adresu portu použitou klientem, který vytváří požadavek na připojení.

veřejná logická hodnota isSSLClient()
slouží k určení, zda je uživatelská procedura volána jako klient SSL/TLS nebo server SSL/TLS. Pokud je vrácena hodnota true, uživatelská procedura se nachází na straně klienta připojení a ověřuje certifikát získaný ze serveru. Pokud se vrátí hodnota false, uživatelská procedura se nachází na straně serveru připojení a ověřuje certifikát odesílaný klientem. Je platné, aby trasa fungoval jako server SSL/TLS a klient SSL/TLS, dešifroval a znovu šifroval provoz. V této situaci, ačkoli existuje jediná výstupní třída, budou některé instance třídy volány jako klienti a některé jako servery. Můžete použít isSSLClient k určení situace pro danou instanci.

public int getConn,ThreadID()
používá se k získání ID pracovního podprocesu, který zpracovává požadavek na připojení, což může být užitečné pro ladění.

veřejný řetězec getChannelNázev ()
Načte název kanálu produktu IBM MQ , který se používá v požadavku na připojení. Tato volba je k dispozici pouze v případě, že příchozí požadavek nepoužívá SSL/TLS a MQIPT vystupuje jako klient SSL/TLS.

veřejný řetězec getQMName()
načítá název správce front IBM MQ použitého v požadavku na připojení. Tato volba je k dispozici pouze v případě, že požadavek klienta nepoužívá SSL/TLS a MQIPT se chová jako klient SSL/TLS.

veřejná logická hodnota getTimedout()
použity uživatelskou procedurou k určení, zda vypršel časový limit.

public IPTCertificate getCertificate()
načte certifikát SSL/TLS, který je třeba ověřit.

public String getExitData ()
načte výstupní data, jak je definuje vlastnost SSLExitData .

veřejný řetězec getExitNázev ()
načte název uživatelské procedury, jak je definován vlastností SSLExitName .

Třída com.ibm.mq.ipt.exit.CertificateExitResponse v produktu MQIPT

Tato třída se používá k předávání informací zpět do produktu MQIPT po ověření certifikátu.

Konstruktory

public CertificateExitOdezva (*int rc*, řetězcová zpráva)

Tento konstruktor může být použit k předání návratového kódu a nějakému textu zprávy. Možné kódy příčiny jsou

- ExitRc.OK.
- ExitRc.CHYBA OVĚŘENÍ
- ExitRc.OVĚŘENÍ PLATNOSTI BYLO ZAMÍTNUTO

public CertificateExitOdezva (*int rc*)

Tento konstruktor může být použit pro předání zpětného návratového kódu bez textu zprávy. Možné kódy příčiny jsou

- ExitRc.OK.
- ExitRc.CHYBA OVĚŘENÍ
- ExitRc.OVĚŘENÍ PLATNOSTI BYLO ZAMÍTNUTO

public CertificateExitResponse ()

Tento konstruktor může být použit k předání zpět návratového kódu ExitRc.OK, bez textu zprávy.

metody

veřejný řetězec getVersion()

Tato metoda vrací verzi této třídy.

veřejný řetězec toString

Tato metoda vrátí řetězcovou reprezentaci odpovědi, například " Kód příčiny: 4, Zpráva: Nezdařila se kontrola CRL.

Třída com.ibm.mq.ipt.exit.IPTCertificate v produktu MQIPT

Tato třída obsahuje certifikát SSL/TLS, který má být ověřen.

metody

public int getVersion()

Tato metoda vrací verzi této třídy.

public byte [] getDerEncoding ()

Tato metoda vrací kódování ASN.1/DER certifikátu X.509 nebo hodnoty NULL, pokud došlo k chybě.

public byte [] getPemEncoding ()

Tato metoda vrací kódování PEM (BASE64) certifikátu X.509 nebo hodnoty NULL, pokud došlo k chybě.

veřejný řetězec getLabel()

Tato metoda vrací jmenovku certifikátu, nebo NULL, pokud došlo 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
```

veřejný řetězec getIssuerName ()

Tato metoda vrátí 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 vrací certifikát podepsaného, nebo hodnotu NULL, pokud není k dispozici. Pro certifikát podepsaný držitelem se vrátí odkaz na sebe sama.

public String toString()

Tato metoda vrací řetězcovou reprezentaci certifikátu.

Třída com.ibm.mq.ipt.exit.IPTTrace v produktu MQIPT

Trasovací funkce produktu MQIPT poskytují vstupní a výstupní volání, která lze použít při vstupu do metody a výstupu z ní. K dispozici jsou také různá data volání pro trasování užitečných informací.

metody

public void entry (String *fid*)

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 příslušnou úrovní odsazení k záznamu bodu, ve kterém tok řízení vstoupí do metody. Toto volání je volitelné, ale pokud se použije, musí být v rámci stejné metody použito odpovídající volání procedury "exit (String)".

public void exit (String *fid*)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody.

Tato metoda zapisuje výstup do výstupního souboru trasování s příslušnou úrovní odsazení k záznamu bodu, ve kterém tok řízení opouští metodu. Tato metoda se používá pouze v případě, že volání "entry (String)" bylo dříve používáno v rámci stejné metody.

public void exit (String *fid*, int *rc*)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody, a *rc* je číselný návratový kód z metody. Tato metoda trasování by měla být použita pro záznam ukončení z metod, které vracejí celé číslo.

Tato metoda zapisuje výstup do výstupního souboru trasování s příslušnou úrovní odsazení k záznamu bodu, ve kterém tok řízení opouští metodu a číselný návratový kód z této metody. Tato metoda se používá pouze v případě, že volání "entry (String)" bylo dříve používáno v rámci stejné metody.

public void exit (String *fid*, boolean *rc*)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody, a *rc* je logický návratový kód z metody. Tato metoda trasování by měla být použita pro záznam ukončení z metod, které vracejí logickou hodnotu.

Tato metoda zapisuje výstup do výstupního souboru trasování s příslušnou úrovní odsazení k záznamu bodu, ve kterém tok řízení opouští metodu a logický návratový kód z této metody. Tato metoda se používá pouze v případě, že volání "entry (String)" bylo dříve používáno 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 zapisuje některá řetězcová data do výstupního souboru trasování.

public void data (String *fid*, int data)

Kde *fid* se používá k identifikaci místa, kde bylo volání provedeno, například název třídy a metody.

Tato metoda zapíše některá celočíselná data 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 zapisuje některá binární data do výstupního souboru trasování.

Ukázka trasování

Chcete-li pomoci při diagnostice problémů v uživatelské proceduře, můžete použít stejné zařízení trasování jako MQIPT, případně můžete implementovat vlastní funkce trasování. Pokud se rozhodnete použít trasovací funkce produktu MQIPT , existují vstupní a výstupní volání, která lze použít při vstupu do metody a výstupu z této metody. Jsou zde také různá data volání pro trasování užitečných informací, jak je zobrazeno v následujícím příkladu.

```
/**
* 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 produktu MQIPT

Návratové kódy, které produkt MQIPT rozpoznává při volání uživatelské procedury certifikátů v řadě různých situací.

Následující návratové kódy jsou rozpoznány produktem MQIPT při volání uživatelské procedury pro potvrzení certifikátu v následujících situacích:

Návratový kód	Popis	Inicializovat	ověřit	Aktualizovat
ExitRc.OK.	Požadavek byl úspěšně dokončen.	yes	yes	yes
ExitRc.CHYBOVÁNÍ_CHYBA	Požadavek na inicializaci selhal, trasa bude zakázána.	yes		
ExitRc.CHYBA_OBNOVENÍ	Požadavek na obnovení selhal, trasa bude zakázána.			yes

Návratový kód	Popis	Inicializovat	ověřit	Aktualizovat
ExitRc.CHYBA OVĚŘENÍ	Ověření platnosti se nezdařilo, požadavek na připojení byl zamítnut.		yes	
ExitRc.OVĚŘENÍ PLATNOSTI BYLO ZAMÍTNUTO	Požadavek na ověření byl odmítnut, požadavek na připojení byl zamítnut.		yes	

LDAP a seznamy odvolaných certifikátů v produktu MQIPT

Produkt MQIPT podporuje použití serveru LDAP (Lightweight Directory Access Protocol) k provedení autentizace seznamu odvolaných certifikátů (CRL) v digitálním certifikátu.

Podpora LDAP byla implementována podobným způsobem jako v produktu IBM MQ, protože stejný server LDAP může být použit jak pro produkt IBM MQ , tak pro produkt MQIPT.

Během navázání komunikace SSL/TLS se vzájemně ověřují spolu s digitálními certifikáty. Ověření může zahrnovat i kontrolu, zda je přijatý certifikát nadále důvěryhodný. Certifikační autority (CA) odvolají certifikáty z různých důvodů, včetně následujících:

- Vlastník byl přesunut do jiné organizace.
- Soukromý klíč již není žádným tajemstvím.

CA publikují odvolané osobní certifikáty v seznamu odvolaných certifikátů (CRL). Certifikáty CA, které byly zrušeny, jsou publikovány v ARL (Authority Revocation List). Nezapomeňte, že následující odkazy na seznamy CRL se také používají u ARL.

Další informace o použití serverů LDAP s produktem IBM MQ a o správě seznamů CRL a ARL naleznete v části Práce s seznamy odvolaných certifikátů a seznamem odvolaných autorit.

MQIPT může podporovat až dva servery LDAP na každé přenosové cestě. První server LDAP je považován za hlavní server s druhým serverem LDAP udržovaný jako záloha. Druhý server se používá pouze tehdy, pokud nelze dosáhnout hlavního serveru. Záložní server by měl být zrcadlovým obrazem hlavního serveru.

Přístup k informacím uloženým na serveru LDAP může být chráněn pomocí ID uživatele a hesla pomocí ID uživatele LDAP a jeho vlastností. Hesla serveru V 9.1.5 LDAP mohou být zašifrována v konfiguraci MQIPT z IBM MQ 9.1.5. Další informace o šifrování hesel používaných produktem MQIPTnajdete v tématu Šifrování uložených hesel.

Když produkt MQIPT načte token PKCS #12 ze souboru svazku klíčů, certifikáty CA se kontrolují na platnost CRL. Pokud má certifikát CA připojený seznam CRL, je zkontrolován, zda jeho platnost vypršela, a pokud ano, bude načten novější seznam CRL ze serveru LDAP. Všechny načtené seznamy CRL budou načteny do aktuálního tokenu a připojeny k jeho certifikátům CA.

Pokud při odeslání dotazu na hlavní server LDAP nejsou k dispozici žádné položky odpovídající danému CA, předpokládá se, že pro tuto CA nejsou žádné seznamy CRL a záložní server se nepoužívá. Avšak pokud nelze dosáhnout hlavního serveru LDAP nebo se nevrátí v daném časovém rámci, použije se záložní server. Jakékoli chyby ze záložního serveru způsobí, že připojení klienta bude ukončeno. Tato akce může být přepsána nastavením vlastnosti **LDAPIgnoreErrors** na hodnotu `true`.

Všechny seznamy CRL načtené pomocí MQIPT se uchovávají v mezipaměti a jsou sdílené všemi připojeními na této přenosové cestě. Pokud platnost CRL cache v paměti cache vypršela, CRL se odstraní z cache a nový se načte ze serveru LDAP. Není-li nový seznam CRL k dispozici, připojení je stále odmítnuto.

Seznam CRL načtený ze serveru LDAP se také kontroluje po vypršení platnosti a zobrazí se varovná zpráva (MQCPW001). RLS s vypršenou platností se stále zavádí do systému a všechny požadavky na připojení odkazující na tento seznam CRL jsou odmítnuty. Měli byste nahradit vypršenou CRL na serveru LDAP aktuální CRL.

Vlastnost **LDAPCacheTimeout** lze použít k řízení toho, jak často se má mezipaměť CRL vymazat. Předvolená hodnota je 1 den. Nastavení této hodnoty na hodnotu 0 znamená, že položky mezipaměti nebudou vymazány, dokud nebude trasa znovu spuštěna.

Seznam odvolaných certifikátů (CRL) může být uložen v souboru svazku klíčů nebo na serveru LDAP. Pokud nový seznam CRL nebyl vydán, další požadavky na připojení jsou odmítnuty. Vyšlou seznamy CRL můžete ignorovat povolením vlastnosti **IgnoreExpiredCRLs** .

Poznámka: Povolíte-li vlastnost **LDAPIgnoreErrors** nebo vlastnost **IgnoreExpiredCRLs** , může být pro vytvoření připojení SSL/TLS použit odvolaný certifikát.

Vlastnosti organizační jednotky pro rozlišující název s více hodnotami v produktu MQIPT

Můžete porovnat více hodnot organizačních jednotek (OU) v rozlišujících názvech certifikátů.

Následující vlastnosti směrování nyní podporují shodu s více hodnotami OU:

- **SSLClientDN_OU**
- **SSLClientSiteDN_OU**
- **SSLServerDN_OU**
- **SSLServerSiteDN_OU**

Chcete-li porovnat více hodnot organizačních jednotek, použijte čárku jako oddělovač v hodnotě vlastnosti přenosové cesty. Příklad:

```
SSLClientDN_OU=Sales, Europe
```

To odpovídá certifikátům s `OU=Sales` i `OU=Europe`. Hodnoty OU se porovnávají ve stejné posloupnosti jako vícenásobné hodnoty organizačních jednotek ve filtrech IBM MQ SSLPEER.

Neuvádějte stejnou vlastnost přenosové cesty více než jednou v sekci `[route]` . Správným způsobem, jak porovnat více hodnot organizačních jednotek, je uvést vlastnost jednou, jak je uvedeno v předchozím příkladu. Zadáte-li stejný atribut více než jednou ve stejné sekci `mqipt.conf` , poslední hodnota se uplatní. Následující položky by například měly za následek pouze shodu s `Evropou` , protože druhá řádka přepíše první:

```
SSLClientDN_OU=Sales
SSLClientDN_OU=Europe
```

Pokud musíte porovnat literálovou čárku uvnitř hodnoty organizační jednotky, vložte zpětné lomítko (\) jako řídicí znak bezprostředně před čárku. Příklad:

```
SSLClientDN_OU=Sales\, Europe
```

Shoduje se s jednou hodnotou: `OU=Sales, Europe`. Zpětné lomítko, které není bezprostředně následováno čárkou, odpovídá literálu zpětného lomítka.

Pokud provádíte upgrade z předchozí verze produktu MQIPT a spoléháte se na schopnost porovnávat čárky v hodnotách organizačních jednotek, musíte do vlastností trasy organizačních jednotek vložit řídicí znaky zpětného lomítka, aby bylo zachováno předchozí chování.

Povolení zamítnutých protokolů a CipherSuites v produktu MQIPT

Zabezpečené protokoly soketů a CipherSuites , které jsou považovány za nezabezpečené, jsou standardně zakázány v produktu Java runtime environment (JRE) dodávaném s produktem MQIPT. Tyto zamítnuté protokoly a CipherSuites musí být povoleny, než je lze použít.

Informace o této úloze

Pokud jste si vědomi potenciálních rizik, ale stále potřebujete použít jeden z protokolů nebo CipherSuites , které jsou považovány za nezabezpečené v produktu MQIPT, postupujte podle této procedury, chcete-li povolit protokol nebo CipherSuite , kterou potřebujete použít.

Postup

1. Upravte soubor `java.security` , který se nachází v adresáři *mqipt_path*`/java/jre/lib/security` , kde *mqipt_path* je umístění, ve kterém je nainstalována funkce MQIPT.
2. Přidejte podporu do prostředí JRE pro protokol nebo algoritmus odebráním příslušné položky ze seznamu zakázaných algoritmů ve vlastnosti `jdk.tls.disabledAlgorithms` .
   - V 9.1.4 Chcete-li přidat podporu pro protokol, odeberte protokol ze seznamu zakázaných algoritmů. Chcete-li například přidat podporu pro TLS 1.0, odeberte produkt TLSv1 ze seznamu.
   - Chcete-li přidat podporu pro sadu CipherSuite, odeberte příslušný algoritmus ze seznamu zakázaných algoritmů. Chcete-li například přidat podporu pro šifrovací sadu SSL_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA , odeberte ze seznamu položku 3DES_EDE_CBC .
3. V 9.1.4
   Chcete-li povolit zabezpečení SSL 3.0 v prostředí JRE, musíte také nastavit systémovou vlastnost `com.ibm.jsse2.disableSSLv3=false`.

   Vlastnost můžete nastavit pomocí proměnné prostředí **MQIPT_JVM_OPTIONS**. Příklad:

   ```
   set MQIPT_JVM_OPTIONS=-Dcom.ibm.jsse2.disableSSLv3=false
   ```
4. Chcete-li povolit zabezpečení SSL 3.0, TLS 1.0nebo TLS 1.1 na trase MQIPT , přidejte odpovídající protokol do vlastnosti směrování **SSLServerProtocols** nebo **SSLClientProtocols** .
5. Restartujte MQIPT , aby se změny vlastností prostředí JRE projevily.

V 9.1.4 Použití kryptografického hardwaru PKCS #11 v příručce MQIPT

Produkt MQIPT může přistupovat k digitálním certifikátům, které jsou uloženy v kryptografickém hardwaru, který podporuje rozhraní PKCS #11 .

Než začnete

Než začnete konfigurovat produkt MQIPT pro použití kryptografického hardwaru, ujistěte se, že jsou šifrovací karty, ovladač karty a všechny přidružené podpůrné softwarty instalovány a řádně fungují.

Podpora kryptografického hardwaru PKCS #11 v produktu MQIPT je poskytována produktem IBM Java PKCS11 Cryptographic Provider (poskytovatelIBMPKCS11Impl). Další informace o poskytovateli IBMPKCS11Impl a seznam šifrovacích karet podporovaných produktem Java 8naleznete v IBM PKCS11 Cryptographic Provider.

Informace o této úloze

Můžete uložit osobní certifikáty a certifikáty CA, k nimž přistupuje produkt MQIPT v úložišti šifrovacích klíčů šifrování. Protože však zařízení PKCS #11 obvykle nemá k dispozici dostatek místa k ukládání velkého množství certifikátů podepisujících subjektů, může být vhodné použít pro certifikáty CA samostatné úložiště klíčů založené na souborech.

Provedením této procedury nakonfigurujete produkt MQIPT tak, aby používal certifikáty v úložišti klíčů kryptografického hardwaru.

Poznámka: Použití kryptografického hardwaru s produktem MQIPT je funkce IBM MQ Advanced . Chcete-li použít tuto schopnost, lokální správce front, který je připojen pomocí trasy MQIPT , je také požadován pro získání nároku IBM MQ Advanced, IBM MQ Appliance nebo IBM MQ Advanced for z/OS VUE .

Postup

1. Vytvořte konfigurační soubor, který se použije při inicializaci poskytovatele IBMPKCS11Impl .

   Stáhněte ukázkové konfigurační soubory pro každou hardwarovou šifrovací kartu, které jsou podporovány poskytovatelem IBMPKCS11Impl , a nakonfigurujte vzorek pro váš systém. Ukázky lze stáhnout z následujícího tématu Java v souboru IBM Documentation: Konfigurační soubor.

   Konfigurační soubor je textový soubor a měl by obsahovat alespoň následující atributy:

   Název
   Přípona názvu instance poskytovatele.

   knihovna
   Plně kvalifikovaný název knihovny PKCS #11 , která se dodává spolu s kryptografickým hardwarem.

   tokenlabel
   Návěští 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 produktu Java , `java.security`, který se nachází v podadresáři `java/jre/lib/security` instalačního adresáře produktu MQIPT .

   a) Pokud se v souboru dosud nenachází, přidejte poskytovatele zabezpečení IBMPKCS11Impl .

   Například přidáním následujícího řádku:

   ```
   security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
   ```

   b) Přidejte úplný název konfiguračního souboru za název poskytovatele.

   Je-li například konfigurační soubor, který jste vytvořili v kroku “1” na stránce 966 , nazván `/opt/mqipt/pkcs11.cfg`, měli byste tuto cestu přidat na stejnou řádku jako poskytovatel zabezpečení:

   ```
   security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /opt/mqipt/
   pkcs11.cfg
   ```

3. Pokud používáte soubor svazku klíčů pro certifikáty CA místo ukládání certifikátů CA do kryptografického hardwaru, vytvořte soubor svazku klíčů CA formátu PKCS #12 .

   Soubor svazku klíčů CA můžete vytvořit buď pomocí grafického uživatelského rozhraní (GUI) **mqiptKeyman** nebo rozhraní příkazového řádku (CLI) produktu **mqiptKeycmd** .

   - Chcete-li použít rozhraní CLI, zadejte tento příkaz:

     ```
     mqiptKeycmd -keydb -create -db filename -pw password -type pkcs12
     ```

     kde *název_souboru* je název souboru klíčového řetězce, 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 nabídku **Soubor databáze klíčů** > **Otevřít**.
     c. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **PKCS11Config**.
     d. Klepněte na tlačítko **OK**. Otevře se okno Otevřít kryptografický token.
     e. Vyberte popisek tokenu šifrovacího zařízení, který chcete použít k ukládání certifikátů.
     f. Do pole **Heslo šifrovacího tokenu** zadejte heslo potřebné pro přístup k kryptografickému hardwaru.

g. Chcete-li vytvořit nový soubor svazku klíčů CA, vyberte volbu **Vytvořit nový soubor databáze sekundárního klíče**.

h. Klepněte na volbu **Typ databáze klíčů** a vyberte volbu **PKCS12**.

i. Do pole **Název souboru** zadejte název souboru svazku klíčů CA.

j. V poli **Umístění** zadejte úplnou cestu k souboru svazku klíčů CA.

k. Klepněte na tlačítko **OK**. Otevře se okno Výzva k zadání hesla.

l. Do pole **Heslo** zadejte heslo pro svazek klíčů CA a zadejte jej znovu do pole **Potvrdit heslo** .

m. Klepněte na tlačítko **OK**.

4. Pomocí produktu **mqiptKeycmd** nebo **mqiptKeyman**požádejte o 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:

-šifrování *název_modulu*
Uvádí plně kvalifikovaný název knihovny PKCS #11 dodané s kryptografickým hardwarem.

-tokenlabel *popisek_tokenů*
Uvádí jmenovku tokenu šifrovacího zařízení PKCS #11 .

-pw *heslo*
Určuje heslo pro přístup k kryptografickému hardwaru.

-label *popisek*
Určuje jmenovku certifikátu.

-size *velikost_klíče*
Určuje velikost klíče. Hodnota může být 512, 1024, 2048, nebo 4096.

-sig_alg *algoritmus*
Uvádí asymetrický podpisový algoritmus použitý pro vytvoření dvojice klíčů položky. The value can be 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_RSA, or SHAWithDSA. Výchozí hodnota je SHA256WithRSA.

-dn *rozlišující_název*
Určuje rozlišující název X.500 uzavřený ve dvojitých uvozovkách.

-file *název_souboru*
Určuje název souboru pro žádost o certifikát.

- Chcete-li použít grafické rozhraní, postupujte takto:

a. V nabídce **Vytvořit** klepněte na **Nový požadavek na certifikát**.

b. Do pole **Jmenovka klíče** zadejte jmenovku certifikátu.

c. Vyberte volbu **Velikost klíče** a **Algoritmus podpisu** , které požadujete.

d. Zadejte hodnoty do pole **Obecný název** a **Organizace**a vyberte volbu **Země**. U zbývajících volitelných polí buď přijměte výchozí hodnoty, nebo zadejte nové hodnoty nebo vyberte nové hodnoty.

e. Do pole **Zadejte název souboru, do kterého chcete uložit žádost o certifikát** , buď přijměte výchozí `certreq.arm`, nebo zadejte novou hodnotu s úplnou cestou.

f. Klepněte na tlačítko **OK**.

g. V seznamu **Požadavky na osobní certifikáty** je zobrazen popisek nové žádosti o osobní certifikát, kterou jste vytvořili. Požadavek na certifikát je uložen v souboru, který jste zvolili.

5. Poté, co certifikační autorita odešle osobní certifikát, přidejte buď certifikát CA do úložiště šifrovacích klíčů, nebo do souboru svazku klíčů CA, pokud již není přítomen.

   - Chcete-li použít rozhraní CLI 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 *název_souboru* je název souboru svazku klíčů CA, *heslo* je heslo svazku klíčů CA, *jmenovka* je jmenovka připojená k certifikátu a *cert_filename* je jméno souboru obsahujícího certifikát CA.

   - Chcete-li použít rozhraní CLI k přidání certifikátu CA do kryptografického 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 systému PKCS #11 dodávaný s kryptografickým hardwarem, *hardwarovým tokenem hardwaru* je jmenovka tokenu šifrovacího zařízení PKCS #11 , *heslo* je heslem pro přístup k kryptografickému hardwaru, *jmenovka* je jmenovka připojená k certifikátu a *název_souboru_certifikátu* 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. Přijmout osobní certifikát poskytnutý CA do úložiště šifrovacích klíčů šifrování.

   - 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 má být přijal, *název_modulu* je úplný název knihovny PKCS #11 dodané s kryptografickým hardwarem, *hardwareční_token* je jmenovka tokenu šifrovacího zařízení PKCS #11 a *heslo* je heslo pro přístup k kryptografickému hardwaru.

     Je-li certifikát CA uložen v klíčovém kruhu CA a nikoli v kryptografickém hardwaru, obdržíte varování, že řetězec certifikátů nelze ověřit, protože příkaz **mqiptKeycmd** nemůže získat přístup k klíčovému svazku CA při přijetí 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 certifikátu a umístění pro nový osobní certifikát, nebo klepněte na tlačítko **Procházet** a vyberte název a umístění.

     c. Klepněte na tlačítko **OK**. Pole **Osobní certifikáty** zobrazuje štítek nového osobního certifikátu, který jste přidali.

7. Zašifrujte heslo pro přístup k kryptografickému hardwaru pomocí příkazu **mqiptPW** .

   V 9.1.5 Zadejte následující příkaz:

```
mqiptPW -sf encryption_key_file
```

kde *encryption_key_file* je název souboru, který obsahuje šifrovací klíč hesla pro vaši instalaci produktu MQIPT . Parametr **-sf** není třeba zadávat, pokud vaše instalace produktu MQIPT používá výchozí šifrovací klíč hesla. Zadejte heslo pro přístup k kryptografickému hardwaru, který má být šifrován při zobrazení výzvy k zadání.

Další informace o šifrování hesel úložiště klíčů najdete v tématu "Šifrování hesla svazku klíčů v produktu MQIPT" na stránce 950.

8. Pokud jste v kroku "3" na stránce 966vytvořili soubor svazku klíčů CA, zašifrujte heslo pro soubor svazku klíčů CA podle pokynů uvedených v kroku "7" na stránce 968.
9. Upravte konfigurační soubor `mqipt.conf` .
   a) Potvrďte, že máte příslušné oprávnění k použití této funkce produktu IBM MQ Advanced nastavením globální vlastnosti **EnableAdvancedCapabilities** na hodnotu `true`.
   b) Povolte použití kryptografického hardwarového úložiště klíčů na trase tím, že nastavíte jednu nebo více vlastností **SSLServerKeyRingUseCryptoHardware**, **SSLServerCAKeyRingUseCryptoHardware**, **SSLServerKeyRingUseCryptoHardware**nebo **SSLServerKeyRingUseCryptoHardware** na hodnotu `true`.

      Další informace o vlastnostech pro povolení použití kryptografického hardwaru na přenosové cestě najdete v tématu Vlastnosti trasyMQIPT.
   c) Používáte-li soubor svazku klíčů pro certifikáty CA, určete umístění svazku klíčů CA nastavením jednoho nebo více vlastností **SSLServerCAKeyRing** nebo **SSLServerCAKeyRing** .

      Pokud jste nakonfigurovali trasu pro použití kryptografického hardwaru pro daný certifikát serveru a neurčujete soubor svazku klíčů CA, použije se kryptografické hardwarové úložiště klíčů jako úložiště klíčů CA.
   d) Uveďte zašifrované heslo pro přístup k kryptografickému hardwaru a svazku klíčů CA pomocí vlastnosti **SSLServerKeyRingPW**, **SSLServerCAKeyRingPW**, **SSLClientKeyRingPW**nebo **SSLClientCAKeyRingPW** .

      V 9.1.5 Nastavte hodnotu vlastností **SSL*KeyRingPW** na šifrovaný výstup hesla pomocí příkazu **mqiptPW** .
   e) Pokud kryptografický hardware obsahuje více než jeden osobní certifikát, určete, který certifikát má být vybrán produktem MQIPT pro odeslání na server SSL/TLS nebo na klienta pro ověření.

      Můžete určit, který certifikát má být vybrán nastavením jedné nebo více vlastností produktu **SSLClientSite*** pro přenosovou cestu klienta SSL/TLS nebo jednu z více vlastností serveru **SSLServerSite*** pro směrování serveru SSL/TLS.

      Další informace o výběru certifikátů z svazku klíčů najdete v tématu "Výběr certifikátů ze souboru svazku klíčů v produktu MQIPT" na stránce 950. Vlastnosti pro výběr certifikátu z svazku klíčů jsou popsány ve vlastnostech MQIPT Vlastnosti přenosové cesty.

V 9.1.5 Chcete-li například použít kryptografické hardwarové úložiště klíčů pro certifikát serveru na přenosové cestě serveru TLS a soubor svazku klíčů k uložení certifikátů CA pro stejnou přenosovou cestu, přidejte do definice předepsané cesty 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

Produkt Java security manager lze použít s libovolnou funkcí produktu MQIPT k zajištění další úrovně zabezpečení.

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 naleznete v tématu Globální vlastnosti produktuMQIPT .

Produkt Java security manager používá dva výchozí soubory zásad:

- Globální soubor se zásadami systému s názvem *$MQIPT_PATH*`/java/jre/lib/security/java.policy` (kde *$MQIPT_PATH* je adresář, kde je nainstalován produkt MQIPT) jsou používány všemi instancemi virtuálního počítače na hostiteli.
- Uživatelem specifický soubor zásad s názvem `.java.policy`, který může existovat v domovském adresáři uživatele.

Lze také použít další soubor zásad MQIPT . Místo předvolených souborů zásad popsaných dříve byste měli použít soubor zásad MQIPT . Další informace viz **SecurityManagerPolicy** v MQIPT globálních vlastnostech .

Syntaxe souboru zásad je poměrně složitá a i když ji lze změnit pomocí textového editoru, je obvykle jednodušší použít obslužný nástroj Policy Tool poskytnutý s produktem Java pro provedení jakýchkoli změn. Obslužný program Policy Tool lze nalézt v adresáři *$MQIPT_PATH*`/java/jre/bin` a je plně zdokumentován v dokumentaci Java.

Ukázkový soubor zásad (`mqiptSample.policy`) byl dodán spolu s produktem MQIPT a ukázal, jaká oprávnění musí být nastavena pro spuštění produktu MQIPT.

Musíte upravit vzorový soubor zásad, aby odpovídal vaší konfiguraci. Konkrétně si všimněte, že domovský adresář produktu MQIPT (umístění souboru mqipt.conf) nemusí být stejný jako instalační adresář produktu MQIPT , takže se při konfiguraci položek FilePermission v zásadě zabezpečení ujistěte, že jste zadali správné adresáře.

Musíte změnit tyto položky:

- Záznam **java.io.FilePermission** , který uděluje přístup pro čtení a zápis k adresáři chyb. Cesta k souboru v této položce se musí odkazovat na domovský adresář produktu MQIPT , protože se zde nachází adresář chyb. Produkt MQIPT v adresáři chyb vytvoří soubory pro zachycení dat FFST (`AMQ*.FDC`) a trasovací soubory (`AMQ*.TRC*`). Je třeba zajistit, aby produkt MQIPT měl oprávnění k vytváření souborů trasování a souborů FFST v adresáři chyb, aby bylo možné odstraňovat problémy s odstraňováním problémů.
- Záznam **java.io.FilePermission** , který uděluje přístup pro čtení a zápis k adresáři protokolů. Cesta k souboru v této položce se musí odkazovat na domovský adresář produktu MQIPT , protože se zde nachází adresář protokolů. Produkt MQIPT vytvoří soubory protokolu připojení (`mqipt*.log`) v adresáři protokolů, je-li povolena globální vlastnost ConnectionLog .
- Záznamy **java.io.FilePermission** , které udělují přístup pro čtení a spuštění 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 produktu MQIPT . Některé z těchto položek lze vynechat, nejsou-li vyžadovány.
- Záznamy **java.net.SocketPermission** musí být upraveny tak, aby kontrolování spojení do každé naslouchající trasy MQIPT . Pro port modulu listener a adresu modulu listener pro každou trasu MQIPT jsou vyžadována oprávnění pro naslouchání a příjem.
- Položky **java.net.SocketPermission** musí být upravovány tak, aby bylo možné řídit připojení mimo každou trasu MQIPT . Oprávnění k připojení se požaduje pro všechny cíle přenosové cesty, servery proxy nebo servery LDAP, ke kterým se trasa MQIPT připojuje. Při zadávání adres s použitím názvu hostitele je vyžadováno oprávnění k vyřešení.

V závislosti na vaší konfiguraci může být také třeba přidat následující položky:

- Položka **java.io.FilePermission** slouží k udělení přístupu pro čtení k souboru mqipt.confnebo k domovskému adresáři produktu MQIPT obsahujícímu soubor mqipt.conf. Potřebujete-li konfigurovat MQIPT vzdáleně pomocí klienta pro administraci, bude produkt MQIPT potřebovat také přístup pro zápis do souboru mqipt.conf , aby mohl uložit změny konfigurace.

- Záznam **java.io.FilePermission** , který má udělit přístup pro čtení k souboru zásad zabezpečení. To je užitečné v případě, že obnova produktu MQIPT způsobí opětovné načtení souboru zásad zabezpečení.
- Některé položky produktu **java.io.FilePermission** mají udělit přístup pro čtení k jakýmkoli souborům svazku klíčů SSL/TLS a souborům pro uložení hesla. To je vyžadováno pouze při použití cesty, která má povoleny vlastnosti SSLClient nebo SSLServer.
- Některé položky produktu **java.io.FilePermission** udělují přístup pro čtení nebo spuštění k libovolným ukončovacím třídám produktu MQIPT . Tato volba je vyžadována pouze v případě, že je povolena uživatelská procedura MQIPT . Možná budete muset udělit dodatečná oprávnění, je-li to vyžadováno uživatelskou procedurou.

Poznámka: Pro každé zpětné lomítko v cestě musí být v položkách Windows **java.io.FilePermission** použity dva znaky zpětného lomítka (\\). Důvodem je to, že jedno zpětné lomítko se používá jako řídicí znak.

Ukázkový soubor předpokládá, že produkt MQIPT byl nainstalován v systému Windows v produktu `C:\Program Files\IBM\MQ Internet Pass-Thru`. Předpokládá také, že domovský adresář produktu MQIPT (umístění souboru `mqipt.conf`) je stejný jako instalační adresář produktu MQIPT .

Pokud jste nainstalovali produkt MQIPT do jiného umístění, je třeba změnit adresář v definici codeBase tak, aby odkazoval na instalační adresář produktu MQIPT . Dávejte pozor, abyste zahrnuli správnou předponu (`file:/`) a správnou příponu souboru (`/lib/com.ibm.mq.ipt.jar`). V systémech UNIX and Linux může být typická adresa URL codeBase `file:/opt/mqipt/lib/com.ibm.mq.ipt.jar`za předpokladu, že je produkt MQIPT nainstalován v produktu `/opt/mqipt`.

Oprávnění jsou obvykle definována se třemi atributy. Chcete-li řídit připojení soketu, jejich hodnoty jsou:

oprávnění třídy
`java.net.SocketPermission`

jméno pro ovládání
To je vytvořeno s formátem `hostname:port`, kde každá komponenta názvu může být uvedena zástupným znakem. Název hostitele může být název domény nebo adresa IP. Pozice levého okraje hostitele může být uvedena hvězdičkou (*). Například `harry.company1.com` by se shodoval s každým z těchto řetězců:

- `harry`
- `harry.company1.com`
- `*.company1.com`
- `*`
- `198.51.100.123` (předpokládá se, že se jedná o adresu IP `harry.company1.com`)

Komponenta portu názvu může být zadána jako jedna adresa portu nebo rozsah adres portu, například:

1414
pouze port 1414

1414-
všechny adresy portů větší než nebo rovné 1414

-1414
všechny adresy portů menší nebo rovné 1414

1-1414
všechny adresy portů mezi 1 a 1414 včetně

povolená akce
Akce použité produktem `java.net.SocketPermission` jsou:

- accept, this allows permission to accept connections from the specified target
- connect, to umožňuje povolení připojit se k zadanému cíli

- listen, to povoluje oprávnění naslouchat na uvedeném portu nebo portech pro požadavky na připojení
- resolve, to povoluje oprávnění používat službu názvů DNS k vyřešení jmen domén na IP adresy

Kontrola produktu Java security manager může být také provedena prostřednictvím systémových vlastností `java.security.manager` a `java.security.policy` Java , ale doporučuje se použít vlastnosti zásad SecurityManager a SecurityManagerpro řízení MQIPT.

Chcete-li zahrnout diagnostické informace do záznamů trasování a FFST , MQIPT musí mít přístup k určitým systémovým vlastnostem a proměnným prostředí MQIPT . Musíte vždy zahrnout následující vlastnosti do zásady zabezpečení produktu Java :

```
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";
```

Pokud nezahrnete všechny tyto vlastnosti, produkt MQIPT nebude fungovat správně a diagnostika problému bude narušena.

Uživatelské procedury zabezpečení v produktu MQIPT

Pomocí uživatelské procedury zabezpečení můžete řídit přístup k cílovému místu určení, jak je definováno vlastností směrování produktu **Destination** . Uživatelská procedura zabezpečení se volá v okamžiku, kdy produkt MQIPT přijme požadavek na připojení od klienta, ale před tím, než učiní připojení k cílovému místu určení.

Na základě vlastností počátečního připojení se uživatelská procedura zabezpečení rozhodne, zda je připojení povoleno dokončit.

Je-li trasa spuštěna, je zavolána uživatelská procedura zabezpečení, aby se inicializovala a aby byla připravena ke zpracování požadavku na připojení. Inicializační proces by měl být použit k načtení všech uživatelských dat a k přípravě těchto dat pro rychlý a snadný přístup, čímž se minimalizuje doba potřebná ke zpracování požadavku na připojení.

Každá cesta může mít svou vlastní 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. Produkt **SecurityExitPath** může také definovat název souboru JAR obsahujícího uživatelskou proceduru zabezpečení definovanou uživatelem.
- Vlastnost **SecurityExitTimeout** se používá v produktu MQIPT k určení, jak dlouho by měla čekat na odpověď z uživatelské procedury zabezpečení při ověření požadavku na připojení.

Podrobnosti o vlastnostech ukončení zabezpečení viz MQIPT Vlastnosti trasy .

Produkt MQIPT používá třídu `SecurityExit` k volání uživatelské procedury zabezpečení definované uživatelem. Tato třída musí být rozšířena uživatelskou procedurou definovanou uživatelem a většina jeho metod je potlačena, aby byla zajištěna požadovaná funkčnost. Objekt `SecurityExitResponse` se používá k předání dat zpět 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 nové místo určení a adresu cílového portu, které slouží k přepsání cesty definované vlastnostmi ukončení zabezpečení.

K dispozici jsou tři ukázkové uživatelské procedury zabezpečení dat, které vám ukážou, jak lze implementovat proceduru zabezpečení.

- Příkaz `SampleSecurityExit` ukazuje, jak lze řídit přístup ke správci front produktu IBM MQ na základě názvu kanálu produktu IBM MQ . Umožňuje pouze připojení s názvem kanálu začínajícím řetězcem "MQIPT." Další informace najdete v tématu Použití uživatelské procedury zabezpečení .
- Produkt `SampleRoutingExit` umožňuje dynamické směrování požadavků na připojení klienta do fondu definovaných serverů produktu IBM MQ . Každý server, který je hostitelem správce front se stejným názvem a se stejnými atributy. Ukázka obsahuje konfigurační soubor, který obsahuje seznam názvů serverů. Další informace naleznete v tématu Směrování požadavků na připojení klienta na servery správce front IBM MQ pomocí uživatelských procedur zabezpečení .
- Produkt `SampleOneRouteExit` umožňuje dynamické směrování na správce front IBM MQ , který je odvozen od názvu kanálu produktu IBM MQ použitého v požadavku na připojení. Ukázka obsahuje konfigurační soubor, který obsahuje mapu názvů správce front k názvům serverů. Další informace najdete v tématu Dynamické směrování požadavků na připojení klienta .

Poznámka: MQIPT běží v jednom prostředí JVM, takže uživatelská procedura zabezpečení definovaná uživatelem může ohrozit normální provoz produktu MQIPT jedním z následujících způsobů:

- Ovlivněné systémové prostředky
- Generovat kritická místa
- Degrade výkon

Měli byste otestovat účinky výstupu zabezpečení rozsáhle před implementací v produkčním prostředí.

Třída com.ibm.mq.ipt.exit.SecurityExit v produktu MQIPT

Tato třída a její veřejné metody musí být rozšířeny pomocí uživatelské procedury zabezpečení definované uživatelem, aby získali přístup k některým společným datům a umožnili, aby se inicializace produktu MQIPT mohla uskutečnit.

Před voláním každé metody produktem MQIPTbudou některé vlastnosti zpřístupněny k použití této metody. Jejich hodnoty mohou být načteny pomocí vhodných metod get definovaných v této třídě.

metody

public int init (IPTTrace)

K dispozici jsou následující vlastnosti:

- port modulu listener
- cíl
- Cílový port
- verze

Inicializační metoda bude volána MQIPT při spuštění přenosové cesty. Při návratu z této metody musí být uživatelská procedura zabezpečení připravena na ověření požadavku na připojení. Platné návratové kódy jsou ExitRc.OK nebo ExitRc.CHYBA INIT_ERROR.

public int refresh (IPTTrace)

K dispozici jsou následující vlastnosti:

- port modulu listener
- cíl
- Cílový port

Metoda refresh bude volána produktem MQIPT , pokud byla požádána o obnovu sama pomocí IPT Administration Client. Tato akce se obvykle volá, když se vlastnost změní v konfiguračním souboru. MQIPT načte všechny vlastnosti z konfiguračního souboru a určí, které z nich byly změněny a zda je třeba trasu okamžitě restartovat, nebo zda může počkat, až se znovu spustí MQIPT .

Tato metoda by měla provést opětovné načtení veškerých externích dat, která používá (tj. data načtená během inicializační metody). Platné návratové kódy jsou ExitRc.OK nebo ExitRc.AKTUALIZACE_CHYBY.

public void close (IPTTrace)
K dispozici jsou následující vlastnosti:

- port modulu listener
- cíl
- Cílový port

Metoda close () bude volána produktem MQIPT , pokud byla požádána o zastavení serverem MQIPT IPT Administration Client. Měl by uvolnit jakýkoli systémový prostředek, který získal během své operace. Produkt MQIPT počká na dokončení této metody před vypnutím.

Tato metoda bude také volána, pokud byla povolena uživatelská procedura zabezpečení, ale nyní byla v konfiguračním souboru zakázána.

public SecurityExitResponse validate (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 ověření bude volána produktem MQIPT , když přijme požadavek na připojení k ověření platnosti. Název kanálu a název správce front nebude k dispozici, pokud byla povolena vlastnost SSLProxyMode , protože tato funkce se používá pouze k tunelování dat SSL/TLS, a proto data obvykle získaná z počátečního datového toku budou nečitelná.

Uživatelská procedura zabezpečení musí vrátit objekt odezvy SecurityExitobsahující následující informace:

- kód příčiny (musí být nastaven)
- new destination address (nepovinné)
- adresa nového portu cílového modulu listener (volitelné)
- zpráva (volitelné)

Kód příčiny určí, zda bude připojení akceptováno nebo odmítnuto produktem MQIPT. Pole portu newDestination a newDestinationmohou být volitelně nastavena pro definování nového cílového správce front. Pokud tyto vlastnosti nenastavíte, budou použity vlastnosti Destination Destination a DestinationPort definované v konfiguračním souboru. Jakákoli zpráva bude připojena k položce souboru protokolu připojení.

Podporované metody pro získání vlastností:

public int getListenerPort ()
načte port modulu listener směrování-jak je definováno vlastností ListenerPort .

veřejný řetězec getDestination()
načte adresu místa určení-jak je definováno vlastností Destination

public int getDestinationPort ()
Načte adresu portu cílového modulu listener-jak je definováno vlastností DestinationPort .

veřejný řetězec getClientIPAddress ()
načítá adresu IP klienta, který vytváří požadavek na připojení

public int getClientPortAddress()
načte adresu portu použitou klientem, který vytváří požadavek na připojení.

public int getTimeout()
načte hodnotu časového limitu. MQIPT bude čekat na ukončení zabezpečení za účelem ověření požadavku-jak je definováno vlastností časového limitu SecurityExit

public int getConn,ThreadID()
načítá ID podprocesu připojení zpracovávající požadavek na připojení, což je užitečné pro účely ladění.

veřejný řetězec getChannelNázev ()
načte název kanálu produktu IBM MQ použitý v požadavku na připojení

veřejný řetězec getQMName()
načítá název správce front produktu IBM MQ použitý v požadavku na připojení

veřejná logická hodnota getTimedout()
může být použit uživatelskou procedurou zabezpečení ke zjištění, zda vypršel časový limit

Třída com.ibm.mq.ipt.exit.SecurityExitResponse

Tato třída se používá k předání odezvy zpět produktu MQIPT z uživatelské procedury zabezpečení definované uživatelem a používá se k určení, zda má být požadavek na připojení akceptován nebo odmítnut. Objekty tohoto typu jsou vytvářeny pouze v metodě ověření (viz "Třída com.ibm.mq.ipt.exit.SecurityExit v produktu MQIPT" na stránce 973). Pro vytvoření těchto objektů existují konvenční konstruktory a existují metody pro každou vlastnost. Další informace naleznete v informacích o uživatelských procedurách zabezpečení.

Vytvoření výchozího objektu odpovědi 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 SecurityExitResponse (int rc, String msg)**
- **public SecurityExitResponse (int rc)**

Metody

public void setDestination(String dest)
nastavuje novou cílovou adresu pro požadavek na připojení

public void setDestinationPort (int port) throws IPTException
nastaví novou adresu portu cílového modulu listener pro požadavek na připojení-vygeneruje výjimku IPTException pro neplatnou adresu portu

public void setMessage(String msg)
přidá zprávu do záznamu protokolu připojení

public void setReasonCode (int rc)
nastavuje kód příčiny pro požadavek na připojení.

Návratové kódy ukončení zabezpečení v produktu MQIPT

Návratové kódy, které produkt MQIPT rozpoznává při volání procedury zabezpečení v řadě různých situací.

Následující návratové kódy jsou rozpoznány MQIPT při volání procedury zabezpečení v následujících situacích:

Návratový kód	Popis	Inicializovat	ověřit	Aktualizovat
ExitRc.OK.	Požadavek byl úspěšně dokončen.	yes	yes	yes
ExitRc.CHYBOVÁNÍ_CHYBA	Požadavek na inicializaci selhal, trasa bude zakázána.	yes		
ExitRc.CHYBA_OBNOVENÍ	Požadavek na aktualizaci se nezdařil.			yes
ExitRc.NEAUTORIZOVÁNO	Ověření platnosti se nezdařilo, 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 produktu MQIPT

Při použití MQIPTje možné omezit rozsah lokálních čísel portů, které se používají při vytváření odchozího připojení.

Nastavte vlastnost **OutgoingPort** na přenosové cestě, abyste uvedli počáteční číslo lokálního portu, a nastavte **MaxConnectionThreads** , abyste uvedli počet portů, které se mají použít. Například, pokud nastavíte **OutgoingPort** na 1600 a **MaxConnectionThreads** na 20, pak se rozsah čísel lokálních portů pro tuto přenosovou cestu bude 1600-1619.

Je na odpovědnosti administrátora produktu MQIPT , aby se ujistil, že mezi cestami nejsou žádné konflikty čísel portů.

Není-li parametr **OutgoingPort** definován, výchozí hodnota 0 znamená, že pro každé připojení je použito systémem přidělené číslo portu.

Při použití protokolu HTTP je počet odchozích portů dvakrát vyšší než při použití protokolu HTTP. V předchozím příkladu, pokud přenosová cesta použila HTTP, rozsah čísel by byl 1600-1639.

Další informace naleznete v tématu Přidělování čísel portů .

Vícecestné systémy

Používáte-li systém s více adresami, můžete určit, která adresa IP se bude vázat pro odchozí připojení, pomocí vlastnosti **LocalAddress** . Názvy hostitelů nejsou v této vlastnosti podporovány.

V 9.1.5 Šifrování uložených hesel v produktu MQIPT

Konfigurace produktu MQIPT může zahrnovat hesla pro přístup k různým prostředkům, stejně jako heslo pro přístup k produktu MQIPT pomocí portu příkazu. V produktu IBM MQ 9.1.5by všechna tato hesla měla být chráněna šifrováním.

Informace o této úloze

Ve verzích starších než IBM MQ 9.1.5mohou být šifrovány pouze hesla, která jsou produktem MQIPT používaná pro přístup k klíčům klíčů nebo kryptografickými hardwarovými úložišti klíčů. Zašifrovaná hesla se ukládají do souborů, na které se odkazují některé z vlastností produktu **SSL*KeyRingPW** . Další hesla pro servery LDAP a heslo pro přístup k produktu MQIPT se ukládají do prostého textu v konfiguračním souboru `mqipt.conf` .

V produktu IBM MQ 9.1.5by veškerá uložená hesla pro použití produktem MQIPT měla být chráněna zašifrováním hesla pomocí příkazu **mqiptPW** . Zašifrovaná hesla se uloží jako hodnoty vlastností v konfiguračním souboru `mqipt.conf` . Produkt MQIPT je schopen rozlišovat mezi zašifrovanými hesly,

prostým textem a názvy souborů v hodnotách vlastností. Měli byste zašifrovat všechna hesla uložená pro použití produktem MQIPT tímto způsobem, protože je to nejbezpečnější metoda ochrany.

Metoda šifrování hesel úložiště klíčů použitých v produktu MQIPT před verzí produktu IBM MQ 9.1.5 je zamítnuta, ale lze ji stále použít. Chcete-li zlepšit ochranu hesel klíčových řetězců, znovu zašifrujte všechna hesla klíčových řetězců, která byla dříve zašifrována, pomocí nejnovější metody ochrany.

Je-li v konfiguraci produktu MQIPT přítomen prostý text nebo slabě chráněné heslo, vydá se varovná zpráva buď při spuštění příkazu MQIPT , nebo při spuštění cesty.

Tento postup slouží k zašifrování hesla, které má být uloženo pro použití produktem MQIPT s použitím nejnovější metody ochrany. Chcete-li zašifrovat heslo svazku klíčů v produktu MQIPT v produktu IBM MQ 9.1.4 nebo dřívější, postupujte podle kroků uvedených v tématu “Šifrování hesla svazku klíčů v produktu MQIPT v produktu IBM MQ 9.1.4 nebo starším” na stránce 978.

Postup

1. Volitelné: Vytvořte soubor obsahující šifrovací klíč hesla, pokud již takový soubor nemáte.

   MQIPT používá šifrovací klíč k zašifrování hesel. 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 klíči šifrování hesel.

   Pokud plánujete spustit produkt MQIPT jako službu, která je automaticky spuštěna, musíte vytvořit soubor s klíči pro šifrování hesel s výchozím názvem `mqipt_cred.key`a umístit jej do domovského adresáře produktu MQIPT .

   Není nutné zadávat šifrovací klíč hesla, je však k tomu bezpečnější. Pokud nezadáte vlastní šifrovací klíč, použije se výchozí šifrovací klíč.

   Poznámka: Musíte se ujistit, že jsou na souboru s klíči šifrování hesla nastavena odpovídající oprávnění k souboru, abyste zabránili neautorizovaným uživatelům číst šifrovací klíč. Pouze uživatel, který spouští příkaz **mqiptPW** , a uživatel, pod kterým MQIPT běží, potřebuje oprávnění ke čtení šifrovacího klíče hesla.
2. Zašifrujte heslo pomocí příkazu **mqiptPW** .

   Syntaxe příkazu **mqiptPW** je popsána v souboru mqiptPW (šifrovat uložené heslo).

   Pokud jste v kroku “1” na stránce 977vytvořili soubor s klíči šifrování hesel, určete název souboru pomocí parametru **-sf** na hodnotu **mqiptPW**. Například lze zadat následující příkaz, který zašifruje heslo pomocí šifrovacího klíče v souboru zadaném argumentem **-sf** :

   ```
   mqiptPW -sf /opt/mqipt/mqipt_password.key
   ```
3. Zadejte heslo, které má být šifrováno při zobrazení výzvy.

   Zašifrované heslo bude výstupem pomocí **mqiptPW**.
4. Okopírujte zašifrované heslo do příslušné vlastnosti v konfiguračním souboru `mqipt.conf` .

   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 977 vytvořili soubor s klíči šifrování hesel s jiným názvem než výchozím názvem, zadejte při spuštění produktu MQIPTnázev souboru s šifrovacím klíčem.

   Při spouštění produktu MQIPTmůžete zadat název souboru s klíči šifrování hesla pomocí parametru **-sf** . Chcete-li například spustit příkaz MQIPT pomocí šifrovacího klíče v souboru zadaném argumentem **-sf** , zadejte následující příkaz:

   ```
   mqipt /opt/mqipt -sf /opt/mqipt/mqipt_password.key
   ```

Informace o jiných metodách zadání názvu souboru s klíči pro šifrování hesla při spuštění produktu MQIPTnaleznete v tématu Zadání šifrovacího klíče hesla.

Šifrování hesla svazku klíčů v produktu MQIPT v produktu IBM MQ 9.1.4 nebo starším

V produktu IBM MQ 9.1.4 a dříve jsou zašifrovaná hesla, která se používají pro přístup k klíčům klíče používaným produktem MQIPT , uložena v souborech. Postupujte podle pokynů v této úloze a zašifrujte heslo svazku klíčů pro použití s produktem MQIPT v produktu IBM MQ 9.1.4 nebo starším.

Informace o této úloze

V produktu MQIPT v produktu IBM MQ 9.1.5používejte namísto této metody více zabezpečené metody ochrany popsané v části “Šifrování uložených hesel v produktu MQIPT” na stránce 976 .

Postup

1. Zašifrujte heslo svazku klíčů pomocí příkazu **mqiptPW** .

   Chcete-li zašifrovat heslo, zadejte následující příkaz:

   ```
   mqiptPW password filename
   ```

   kde:

   Password
   je heslo pro přístup ke svazku klíčů pro přístup k souboru svazku klíčů je prázdné.

   Filename
   je název souboru hesel, který má být vytvořen

   Syntaxe příkazu **mqiptPW** je popsána v souboru mqiptPW (šifrovat uložené heslo).
2. Nastavte odpovídající vlastnost přenosové cesty na název souboru, který obsahuje zašifrované heslo, které bylo vytvořeno v kroku “1” na stránce 978.

   Chcete-li například určit 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 pomáhají návrháři vybudovat zabezpečené řešení.

- Pokud se v interní síti nachází mnoho klientů, kteří se snaží vytvořit odchozí připojení, mohou všechny procházet MQIPT umístěnými uvnitř brány firewall. Administrátor brány firewall pak musí udělit externí přístup pouze k počítači s produktem MQIPT .
- Produkt MQIPT se může připojit pouze ke správcům front, pro které byl explicitně nakonfigurován v jeho konfiguračním souboru, pokud MQIPT nevystupuje jako server proxy SOCKS nebo nepoužívá uživatelskou proceduru zabezpečení.
- MQIPT ověřuje, zda jsou zprávy, které přijímá a vysílají, platné a jsou v souladu s protokolem IBM MQ . To pomáhá zabránit tomu, aby byl produkt MQIPT používán pro bezpečnostní útoky mimo protokol IBM MQ . Pokud příkaz MQIPT vystupuje jako server proxy SSL/TLS, až budou zašifrována všechna data a protokoly produktu IBM MQ , může produkt MQIPT zaručit pouze počáteční navázání komunikace SSL/TLS. V této situaci použijte Java security manager.
- Produkt MQIPT umožňuje uživatelským procedurám kanálu spouštět své vlastní protokoly zabezpečení koncových uživatelů.
- Celkový počet příchozích připojení můžete omezit nastavením vlastnosti `MaxConnectionThreads` . To pomáhá chránit zranitelného interního správce front před útoky typu zamítnutí služby.

Konfigurační soubor

Musíte chránit konfigurační soubor MQIPT , `mqipt.conf`, ze čtení neautorizovanými uživateli, protože může obsahovat citlivé informace, jako například heslo **AccessPW** , které řídí vzdálený administrativní přístup k MQIPT. Chránit všechna hesla zadaná v konfiguračním souboru podle postupu uvedeného v tématu "Šifrování uložených hesel v produktu MQIPT" na stránce 976. Také se ujistěte, že `mqipt.conf` je chráněn proti neautorizované modifikaci. Nastavte oprávnění k souboru operačního systému pro produkt `mqipt.conf` tak, aby mohl soubor číst nebo aktualizovat pouze uživatelský účet, který spouští produkt MQIPT .

Příkazový port

Port příkazu MQIPT přijímá řídicí příkazy vydané skriptem **mqiptAdmin** nebo IPT Administration Client. Je-li povolen port příkazu MQIPT , je třeba zabránit neoprávněnému přístupu k němu. Zejména je-li povolena vlastnost **RemoteShutdown** , mohl by vzdálený uživatel ukončit práci MQIPT.

Měli byste použít bránu firewall k omezení sady počítačů, které se mohou připojit k portu příkazu MQIPT . Také byste měli nastavit heslo pro řízení přístupu k portu příkazu pomocí vlastnosti **AccessPW** .

Poznámka: Připojení k portu příkazu MQIPT nejsou šifrována. Data odeslaná přes síť, včetně hesla, by mohla být viditelná pro ostatní uživatele v síti.

Než povolíte port příkazu, musíte ohodnotit rizika, která umožní vzdálenou administraci produktu MQIPT . Pokud je port příkazu povolen, zvažte vypnutí vzdáleného ukončení práce se vlastností **RemoteShutdown** .

Protokoly připojení v produktu MQIPT

Produkt MQIPT poskytuje protokolovací zařízení, které obsahuje seznamy všech úspěšných a neúspěšných pokusů o připojení.

Je řízen pomocí vlastností **ConnectionLog** a **MaxLogFileSize** . Další informace naleznete v tématu Globální vlastnosti produktuMQIPT .

Při každém spuštění produktu MQIPT se vytvoří nový protokol připojení. Pro identifikaci obsahuje název souboru aktuální časové razítko, například:

```
mqiptYYYYMMDDHHmmSS.log
```

kde:

YYYY je rok
MM je měsíc
DD je den
HH jsou hodiny
mm je minuta
SS jsou sekundy

Když protokol připojení dosáhne maximální velikosti určené vlastností **MaxLogFileSize** , vytvoří se záložní soubor `mqipt001.log`. Je udržováno maximálně dva záložní soubory (`mqipt001.log` a `mqipt002.log`).

Záznam v protokolu připojení představuje každou část žádosti o připojení. Požadavek na připojení přijatý produktem MQIPT a výsledné nové připojení, které MQIPT učiní na cílovou adresu, se zobrazí jako dva záznamy protokolu a následně dva další záznamy, když je každé spojení ukončeno.

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'
```

Konfigurace produktu IBM MQ Internet Pass-Thru pomocí kontejnerů

V kontejneru můžete spustit IBM MQ Internet Pass-Thru (MQIPT). Základní obraz použitý kontejnerovým obrazem musí používat podporovaný operační systém Linux.

Procedura

- Ukázkový obraz produktu MQIPT Docker je k dispozici v úložišti mq-container GitHub . Chcete-li sestavit a spustit kontejner, postupujte podle pokynů v části IBM MQ Internet Pass-Thru na systému Docker.

Jak pokračovat dále

Spuštěný kontejner můžete zobrazit pomocí příkazu **docker ps** . Chcete-li zobrazit výstup konzoly serveru MQIPT spuštěného v kontejneru Docker , použijte příkaz **docker logs ${CONTAINER_ID}** .

Poznámky

Tyto informace byly vyvinuty pro produkty a služby poskytované v USA.

Společnost IBM nemusí nabízet produkty, služby nebo funkce uvedené v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou ve vaší oblasti aktuálně dostupné, získáte od místního zástupce společnosti IBM. Odkazy na produkty, programy nebo služby společnosti IBM v této publikaci nejsou míněny jako vyjádření nutnosti použití pouze uvedených produktů, programů či služeb společnosti IBM. Místo toho lze použít jakýkoli funkčně ekvivalentní produkt, program nebo službu, které neporušují žádná práva k duševnímu vlastnictví IBM. Ověření funkčnosti produktu, programu nebo služby pocházející od jiného výrobce je však povinností uživatele.

Společnost IBM může vlastnit patenty nebo nevyřízené žádosti o patenty zahrnující předměty popsané v tomto dokumentu. Vlastnictví tohoto dokumentu neposkytuje licenci k těmto patentům. Dotazy týkající se licencí můžete posílat písemně na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Odpovědi na dotazy týkající se licencí pro dvoubajtové znakové sady (DBCS) získáte od oddělení IBM Intellectual Property Department ve vaší zemi, nebo tyto dotazy můžete zasílat písemně na adresu:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE" , BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás toto omezení nemusí vztahovat.

Uvedené údaje mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené jsou pravidelně upravovány a tyto změny budou zahrnuty v nových vydáních této publikace. Společnost IBM může kdykoli bez upozornění provádět vylepšení nebo změny v produktech či programech popsaných v této publikaci.

Veškeré uvedené odkazy na webové stránky, které nespravuje společnost IBM, jsou uváděny pouze pro referenci a v žádném případě neslouží jako záruka funkčnosti těchto webů. Materiály uvedené na tomto webu nejsou součástí materiálů pro tento produkt IBM a použití uvedených stránek je pouze na vlastní nebezpečí.

Společnost IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vyžádání vašeho svolení.

Vlastníci licence k tomuto programu, kteří chtějí získat informace o možnostech (i) výměny informací s nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) oboustranného využití vyměňovaných informací, mohou kontaktovat informační středisko na adrese:

IBM Corporation
Koordinátor spolupráce softwaru, oddělení 49XA
148 00 Praha 4-Chodby

148 00 Praha 4-Chodov
U.S.A.

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek smlouvy IBM Customer Agreement, IBM International Program License Agreement nebo jiné ekvivalentní smlouvy mezi námi.

Jakékoli údaje o výkonnosti obsažené v této publikaci byly zjištěny v řízeném prostředí. Výsledky získané v jakémkoli jiném operačním prostředí se proto mohou výrazně lišit. Některá měření mohla být prováděna na vývojových verzích systémů a není zaručeno, že tato měření budou stejná i na běžně dostupných systémech. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky mohou být jiné. Čtenáři tohoto dokumentu by měli zjistit použitelné údaje pro své specifické prostředí.

Informace týkající se produktů jiných výrobců pocházejí od dodavatelů těchto produktů, z jejich veřejných oznámení nebo z jiných veřejně dostupných zdrojů. Společnost IBM tyto produkty netestovala a nemůže potvrdit správný výkon, kompatibilitu ani žádné jiné výroky týkající se produktů jiných výrobců než IBM. Otázky týkající se kompatibility produktů jiných výrobců by měly být směrovány dodavatelům těchto produktů.

Veškerá tvrzení týkající se budoucího směru vývoje nebo záměrů společnosti IBM se mohou bez upozornění změnit nebo mohou být zrušena a reprezentují pouze cíle a plány společnosti.

Tyto údaje obsahují příklady dat a sestav používaných v běžných obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob a názvy společností, značek a produktů. Všechna tato jména a názvy jsou fiktivní a jejich podobnost se jmény, názvy a adresami používanými ve skutečnosti je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly plně testovány za všech podmínek. Společnost IBM proto nemůže zaručit spolehlivost, upotřebitelnost nebo funkčnost těchto programů.

Při prohlížení těchto dokumentů v elektronické podobě se nemusí zobrazit všechny fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Informace programátorských rozhraní, je-li poskytnuta, vám pomohou vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, které umožňují zákazníkům psát programy za účelem získání služeb produktu WebSphere MQ.

Tyto informace však mohou obsahovat i diagnostické údaje a informace o úpravách a ladění. Informace o diagnostice, úpravách a vyladění jsou poskytovány jako podpora ladění softwarových aplikací.

Důležité: Nepoužívejte tyto informace o diagnostice, úpravách a ladění jako programátorské rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM , ibm.comjsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek IBM je k dispozici na webu na stránce "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Ostatní názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností.

Microsoft a Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Tento produkt obsahuje software vyvinutý v rámci projektu Eclipse Project (http://www.eclipse.org/).

Java a všechny ochranné známky a loga založené na termínu Java jsou ochranné známky nebo registrované ochranné známky společnosti Oracle anebo příbuzných společností.

Číslo položky:

(1P) P/N: